DOCUMENT RESUME

ED 457 932 JC 010 690

AUTHOR	DeLisse, Regina L.
TITLE	Rationale for Computer Ethics Policies and a Model Policy for the North Carolina Community College System.
PUB DATE	2000-08-00
NOTE	276p.; Doctoral Dissertation, University.
PUB TYPE	Dissertations/Theses - Doctoral Dissertations (041)
EDRS PRICE	MF01/PC12 Plus Postage.
DESCRIPTORS	*Administrator Attitudes; *Community Colleges; Computer Uses in Education; *Educational Technology; *Ethical Instruction; *Ethics; Privacy; *Student Behavior; Two Year Colleges
IDENTIFIERS	*North Carolina Community College System

ABSTRACT

This study addresses new concerns of higher education organizational leaders as a result of the extended use of information technology on college campuses. Some of the most important and controversial issues include ethical and legal matters such as privacy, freedom of speech, intellectual property, and legislative attempts for Internet regulation. A survey of community college administrators and system administrators in the North Carolina Community College System was conducted. This survey was designed to explore the extent to which various unethical or antisocial incidents have occurred in computer labs or elsewhere on the campuses, and to solicit input in the development of computer ethics policies and an ethical instruction plan. Twenty-four out of the 58 invited system administrators participated in the survey (response rate 41%). Survey findings support implementing ethics instruction on campus. A model computer ethics policy and accompanying instructional plan is presented with this study as a practical solution to technology-induced dilemmas for organizational leaders within higher education. This document also reviews perspectives on ethics and computer ethics. Behavioral theories, particularly the Theory of Deindividualization, are highlighted to illuminate underlying assumptions and behavioral intentions of computer users and are used to develop a set of computer ethics policies and procedures. (Contains 168 references.) (GC)

Reproductions supplied by EDRS are the best that can be made
from the original document.

ED 457 932

Rationale for Computer Ethics Policies and a Model Policy For the North Carolina Community College System

Regina L. DeLisse

Regent University

August 2000

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☑ This document has been reproduced as received from the person or organization originating it

☐ Minor changes have been made to improve reproduction quality

- Points of view or opinions stated in this document do not necessarily represent official OERI position or policy

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

Regina DeLisse

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

JC010690

BEST COPY AVAILABLE

Center for Leadership Studies
Regent University

This is to certify that the dissertation prepared by:

Regina L. DeLisse

Entitled

RATIONALE FOR COMPUTER ETHICS POLICIES AND A MODEL POLICY FOR THE NORTH CAROLINA COMMUNITY COLLEGE SYSTEM

Has been approved by her committee as satisfactory completion of the dissertation requirement for the degree of Doctor of Philosophy

J. D. Keeler 10-28-00
Dr. Jack Keeler, Committee Chair, College of Communication and Arts Date

10 24 00
Dr. Alan Arroyo, Committee Member, School of Education Date

William Cox 10/24/00
Dr. William Cox, Committee Member, School of Education Date

Kathaleen Reid Martinez 10/25/00
Kathaleen Reid-Martinez, Ph.D., Dean, Center for Leadership Studies, Date

Abstract

The purpose of this study is to address new sets of issues and potential concerns of organizational leaders within higher education due to the prominence of computers on college campuses. Many of these technology-induced issues involve economic, political, social, operational, and other factors; however, the most important and controversial issues often deal with such legal and ethical matters as security, privacy, and other matters. An emphasis is placed upon the clarification, identification, and confirmation of the practical problems and apprehension regarding computer ethics facing organizational leaders within higher education. Using survey research, insight is provided regarding the extent to which and how college administrators and system administrators within the North Carolina Community College System have dealt with issues of computer ethics and computer ethics policies on their campuses. Behavioral theories, particularly the Theory of Deindividuation, are used to describe the underlying assumptions and behavioral intentions of computer users and serve as a theoretical framework to assist in the development of computer ethics policies and procedures. A model computer ethics policy and accompanying instructional plan and recommendations are presented. These are based on a more comprehensive understanding of key ethical issues and problems and are rooted in significant behavioral assumptions. The policy and instructional plan are proposed as a practical solution to technology-induced ethical dilemmas for educational leaders searching for one.

Table of Contents

Abstract ii

Chapter I: Rationale for Computer Ethics Policies and a Model....... Policy for The North Carolina Community College System 1
  Computers and Society 1
  Behavioral Models 6
  Special Needs for Computer Ethics and Policies in Community College Systems 8
  North Carolina Community College System 12
  Purpose of Study 14
  Scope and Importance of Study 17

Chapter II: Review of Literature 19
  Computers and Their Ethical Impact on Society 20
  Fundamental Ethical Perspectives 22
    Philosophical perspectives 22
    Perspectives on computer ethics 24
    Computer ethics versus computer laws 27
  Legal Issues 29
    Privacy 29
    Freedom of speech (censorship) 31
    Intellectual property (copyright issues) 34
    Legislative attempts to regulate the Internet 35
  Development of the Computer Ethics Field 38
    History, definition, and contributors 39
    Professional codes of ethics/standards 41
  Business Ethics/Organizational Leadership........ 44
  Computer Ethics in Education 48
    Student ethical perceptions 49
    Concerns of educators of the Internet 54
    Ethics instruction and education 55
    Responsibility for ethics instruction 56
    Ethics in other disciplines 58
    Teaching of ethics in computer science 59
    Ethics instruction 64
    Impact of a policy 66
  Behavioral Models 74
    Fishbein Behavioral Intention Model 74
    Theory of Reasoned Action 75
    Theory of Planned Behavior 76
    Theory of Deindividuation 77
    Deindividuation and computers 89
  Summary 98

Chapter III: Methodology 101
    Survey Participants 103
    Design and Procedure 104
    Materials 106

Chapter IV: Results of College Administrator Survey 108
    Purpose of the Survey 108
    Respondents 109
    Administrators Perceptions of the Extent of Computer Ethics Problems on their Campuses 109
    Growth of Computer Ethics Issues 113
    Perceived Need for and Communication of a Computer Use Policy 114
    Need for Computer Ethics Instruction and Enforcement of Policies 115
    Application of the Theory of Deindividuation 117
    Model Computer Ethics Policy and Ethical Instruction Plan 121

Chapter V: Discussion 127
    Research Questions and Main Findings 130
    Interpretation and Comparison to Past Research Findings 135
    Contributions of the Survey Research 144
    Limitations of the Survey 145

Chapter VI: Model Computer Ethics Policy and Instructional Plan 149
    Rationale for a Computer Ethics Policy 149
    Proposed Policy 151
        Policy development guidelines 151
        Sample policies examined 152
        Particular needs of community colleges 153
        Symbolic role of North Carolina community colleges 154
        Application of Theory of Deindividuation 154
        System administrator input and policy changes 155
    Proposed Instructional Plans 159
        Importance of ethical instruction 159
        Teaching approaches in computer ethics 161
        Suggested ethics instruction modules 162
    Other Recommendations 165
        Implementation guidelines 166
        Campus culture 169
        Contributions of the study 169
        Directions for future research 171
    Summary 173

References 175

Appendices 193
A: Fishbein's Behavioral Intention Model 193

B: Theory of Planned Behavior 194
C: Theory of Deindividuation 195
D: North Carolina Integrated Information Network Policy 197
E: North Carolina Community Colleges 200
F: Introductory Packet Materials 206
G: Research Packet Cover Letters 209
H: Research Packet Materials 212
I: Means And Standard Deviations: Arranged By Research Questions 227
J: Appropriate Use Policy: Durham Technical Community College Computing Resources 233
K: Computer Ethics Syllabi Samples 235
L: Sample Computer Ethics Policies Examined 245
M: Revised Model Computer Ethics Policy And Instructional Plan 254

Chapter I: Rationale for Computer Ethics Policies and a Model Policy for the North Carolina Community College System

Due to the tremendous growth and utilization of information technology, many college campuses are experiencing new sets of issues and potential concerns. While many of these technology-induced issues involve economic, political, social, operational, and other factors, the most important and controversial issues are often legal and ethical matters dealing with security, privacy, and many other considerations. Vitell and Davis (1990) suggest that the academic and professional fields currently experiencing the most ethical problems and conflicts are finding that many of these difficulties are associated with information systems. This is due in part to the relatively young, rapidly changing nature of information technologies, their applications and their increasingly pervasive presence.

Computers and Society

The prominence of information technologies resulting in dependence on computers as necessary tools has penetrated all of society, including the education field and its institutions of higher learning. However, the speed at which technological advancements have progressed appears to have been far faster than consideration of their impact upon societal or cultural norms and values or the development of norms governing the use of the technologies. In addition, these new technologies have caused new ethical and legal questions to emerge. "Information technology represents skills and tools of such power (and yes, even glamour) so that some argue that it makes unique ethical claims and triggers distinct notions about right and wrong" (Lewis, 1993, p. 46).

While utilizing and harnessing information technology of numerous types has brought various ethical issues, many of these have focused on and been unique to the Internet and its ability to connect individuals, including those on college campuses, to the world. Some of the key areas of ethical concern that have been raised include: accessing without authorization; engaging in software piracy; illegal copying of licensed software; infringing upon software license agreements; knowingly transmitting or creating computer viruses; intercepting transmitted information; hacking into the network and system; engaging in the displaying, downloading, and viewing of inappropriate, offensive, or obscene materials; and finally, misrepresenting the college on the Internet and/or posting information on the Internet that violates university codes of conduct.

An InformationWeek/Ernst & Young survey of 1,290 information system executives showed that one in five companies suffered break-ins and attempted break-ins via the Internet. The actual number could be higher due to the fact that only half felt they would be able to detect a break-in from the Internet. Break-ins are occurring in spite of security. Seventy percent of the companies surveyed have break-in protection, 60% with virus protection and passwords, and 15% with encryption, or encoding of data so that it may not be read by unauthorized individuals (Violino, 1996).

A statistic that many would find alarming indicates that there are an estimated 72,000 pornographic sites on the Internet with approximately 39 new sites appearing daily ("US Senator Dan Coats," 1997). The Washington Post has declared the Internet the "largest pornography store in the history of mankind ("US Senator Dan Coats," 1997). However, many organizations and elements of society have declared this is a cost of maintaining freedom of speech and freedom of press rights. For example, the American Library Association (ALA) has insisted that we must not prohibit children from accessing any items while refusing to give parents access to their minor children's borrowing records. Judith Krug, chief spokesperson for the ALA, states there is to be no access limit regardless of content or age of user. She further commented that blocking material leads to censorship. "That goes for pornography and bestiality too. If you don't like it, don't look at it" (Washington Transcript Service, 1997).

Even more alarming to many people is the fact that individuals can buy or freely access almost anything on the Internet, from do-it-yourself guns, explosive recipes, poison promoted under the guise of helping elderly people end their lives, and much more. One child was arrested recently for buying Web access with stolen credit card numbers. Only, he did not steal them; generated them from a mathematical equation downloaded from a hacker's Web site. One on-line publisher "Loompanics" distributes manuals: Escape from Controlled Custody; Murder, Death & Torture; Drugs; and Bombs & Explosives. Multiple disclaimers stating that they do not advocate breaking the law prevent legal implications (PC Computing, 1999). As Larrabee (1994) concludes, there is a thriving underground market where everything from "pipe bomb recipes" to "kiddie porn" is shared.

Ethical questions about the Internet also have led to greater attention, concern, and debate in the legal arena about the Internet and uses of computers and other information technologies as a whole. Such legal issues as privacy, liability, copyright, property rights, accuracy of information, and accessibility factors are among many currently being raised and discussed.

As leaders in all fields have approached these technology-related, ethical dilemmas and new legal issues—often with little or no guidance and forethought—many have turned to existing governmental and legal measures that may be capable of settling disputes and establishing guiding restraints. Anderson (1996), however, argues that current laws relating to various crimes are outdated and confusing because they were not written for technologies of today. For example, several legal attempts in the United States to regulate the Internet have met with bitter debate concerning First Amendment Rights. Laws are created, but they are repeatedly declared unconstitutional by individuals and groups proclaiming protection of freedom of speech. As a result, legal measures continue to provide little relief to ethical dilemmas.

Legal measures that have been attempted to eliminate problems include such bills as the Internet School Filtering Act of 1998 sponsored by Senators McCain and Hollings, and the Communications Decency Act sponsored by Senators Exxon and Coats. In spite of good intentions, The Internet School Filtering Act requires only one computer in each school to be equipped with blocking software, and the Supreme Court struck down the Communications Decency Act in 1997 as unconstitutional. Given this lack of legal support, strong ethics policies, procedures, and instruction appear to be the only viable solutions to our present rampage of concerns, issues, and dilemmas.

It is leaders of organizations of all types who are being challenged most by ethical issues related to information technologies generally and computers and the Internet specifically. Organizational leaders within higher education, in particular, have struggled with the increasing ethical demands of information technology. For the most part, educators at all administrative levels are affected; however, system administrators are particularly concerned. System administrators must continually monitor campus computing situations in search of possible infractions and subsequent solutions due to misuse, either intentional or unintentional, by system users.

Many negative consequences and issues have arisen as a result of educational uses of computer technologies, only to be apparently pushed aside or ignored for the positive aspects, the power, and the appeal of the latest "new" thing that can be accomplished. For example, schools may be liable for personal injury or property damage caused by student actions or communications involving district-run computer networks. As such, if a student distributes defamatory statements over the network, the school could be considered a publisher under libel law holding the educational institution legally liable (Sivin & Bialo, 1992).

Educational leaders have tended to be dazzled by the technologies or have been pressured to "keep up" with trends in their use or application. As a result, they may have made decisions without properly planning for and understanding the ethical problems that have come with their use and application. Moreover, inadequacies of ethical codes and teaching about ethical issues become even more apparent in today's controversial and constantly changing technological environment. In this environment, new ethical dilemmas are created, and acting wrongfully becomes easier (Rubin, 1996). Again, as many have observed, "Ethics problems will continue to evolve because of the revolutionary advance of computer technology and an ever-changing society" (Day & Day, 1996, p. 60).

Educational leaders must address these ethical issues because they have a unique opportunity to help educate computer users to make the best moral decisions. Kizza (1996) suggests the long-term solution is education. Sivin and Bialo (1992) add further support by suggesting that schools cannot depend on parents to provide guidance concerning information technology when many parents have insufficient experience in this area. They may not fully understand the ethical and legal issues; therefore, schools must provide guidance and instruction. What some students will learn in this respect will influence their uses of computers, the Internet, and other technologies long after they leave the college environment and will certainly prove beneficial to them and the college or university as a whole.

The basic dilemma for institutions of higher education is to find a way to satisfy the need for freedom of information access and dissemination and, at the same time, accommodate the various conflicting social values of their diverse communities. Educational institutions must solve this problem, and at the same time, establish policies that can adapt to rapid innovations in information technology (Day & Day, 1996).

Behavioral Models

According to the literature reviewed, few theories are sufficiently applicable to the study of computer user behavior and ethics. Among the few theories identified by scholars as valid tools for the study of computer ethics are the theories of Reasoned Action, Planned Behavior, and Deindividuation. These theories may assist educational leaders in understanding the underlying factors involved in unethical behavior. They are based on considerable research that might be incorporated into or serve as a framework higher education leaders could use in developing computer ethics policies and ethical instruction.

To develop and implement an effective computer ethics policy, it seems essential that educational leaders must consider the behaviors they are attempting to change. A better understanding of behavior can lead to a computer ethics policy that actually facilitates ethical behavior in computer users rather than displaying a fixed set of rules that tend to be undervalued or ignored by the computer user. As one observer of the impact of computers noted, "The computer has affected the whole of society. People, however, are often puzzled by the nature and the origin of its effects. A computer is often seen as a 'disembodied other,' responsible for all sorts of autonomous behavior" (Grabow, 1996, p. 298). Most respondents, according to a recent survey, strongly agreed that they valued being able to visit sites on the Internet anonymously (Connolly, 1997). Information technology removes us from concrete object—the perpetrator believes he can escape detection (Sivin & Bialo, 1992). Information technology also creates psychological distance (Friedman, 1990). Without being face to face with another individual, we may not think about in advance or fully experience the effect of unethical acts. In fact, we may not experience the victim as a person at all (DeMaio, 1990, 1991).

Based upon the impact on behavior by information technology and vice versa, examination of behavioral theories appears appropriate. One behavioral theory that appears to offer a particularly promising framework for developing computer ethics policies, procedures, and instruction on college campuses is the Theory of Deindividuation (Festinger, Pepitone, & Newcomb, 1952; Zimbardo, 1969).

"Deindividuation" is a process in which a "series of antecedent social conditions lead to changes in perception of self and others, and thereby, to a lowered threshold of normally restrained behavior. Under appropriate conditions what results is the release of behavior in violation of established norms of appropriateness" (Zimbardo, 1969, p. 251).

Festinger et al. (1952) first defined the term "deindividuation" to refer to situations where abnormal and antisocial behavior is released in groups in which individuals are not seen or paid attention to as individuals (p. 382). More recent applications of deindividuation include the study by Dodd (1985) that demonstrated the concept of deindividuation and revealed that "normal, well-adjusted" college students are capable of inappropriate, antisocial behavior in certain situations (Dodd, 1985, p. 89). Kiesler, Siegel, and McGuire (1984) found that computer-mediated communication offers some of the same conditions important for deindividuation—anonymity, reduced self-regulation, and reduced self-awareness. In a similar study, it was found that "submergence in a technology, and technologically-induced anonymity and weak social feedback might also lead to feelings of loss of identity and uninhibited behavior" (Siegel et al, 1986, p. 183).

The reason that perhaps the Theory of Deindividuation may be well-suited for developing computer ethics policies, procedures, and instruction on college campuses is based upon the nature of the computer and associated underlying behavior. When developing policies, procedures, and instructions, it is critical to fully understand motivating factors and underlying behavior. This theory is one of the few behavioral theories identified by scholars as useful in understanding motivational forces that facilitate computer user behavior and takes into consideration both personal and social identity.

Special Needs for Computer Ethics and Policies in Community College Systems

The community college offers a unique opportunity for educational administrators and scholars concerned about ethics to instruct and inform computer users. There is a need for research by scholars focusing upon the impact of information technology and clarity of ethical implications caused by computer usage. Community colleges are very prominent users of computers and providers of computer instruction. They serve diverse and numerous elements of the population and publics. Ethical issues are particularly important given the responsibility that community colleges have concerning the general welfare of the public they serve. As communities increasingly rely and depend on information technology, there is a greater need for awareness of ethical issues and far-reaching implications related to computing. Based upon the growing importance of community colleges and the opportunity to reach a larger, more diverse student population, this educational system is worthy of further investigation.

The community college has a diverse student population more reflective of and better representing the adult population. The community college serves a broader sector of local population than any other higher education institution (Cohen & Brawer, 1996). Community colleges serve 46% of all African-American students in higher education, 55% of all Hispanic students, 46% of all Asian/Pacific Islander students, 55% of all Native-American students, as well as 46% of first-time freshmen (AACC, 1998). The community college also serves special populations using technology. Special populations include the homebound, senior citizens, prisoners, non-English-speaking students, and physically and mentally challenged students (North Carolina Community College System, 1999).

The community college has the opportunity to reach greater numbers of the population. The highest growth has occurred in two-year colleges as compared to four-year universities. Between 1965 and 1996, two-year colleges increased in total fall enrollment by 474% as compared to four-year institutions of higher education, which increased only 185% (US Department of Education Statistics, 1998). Recent statistics show that 10.4 million students have enrolled within the 1,132 community colleges in the United States (AACC, 1998).

> The community college has been the nation's primary site of access to higher education. More students have enrolled in community colleges than in any other sector of American higher education. The enormous enrollment growth in the higher education enterprise, to which Americans frequently point with pride, could not have occurred without the community college. (Eaton, 1994, p. xi)

Community colleges have the potential to impact society at a greater level than many other educational institutions. They help individuals learn what they need to be effective, responsible societal members and best provide a "channel of upward mobility to individuals of any age" (Cohen & Brawer, 1996, p. 408). Community colleges lead in offering welfare reforms and increased literacy levels.

Forty-eight percent of community colleges offer welfare-to-work programs (AACC, 1998). Societal impacts within the community by the college include: increased social mobility, cost benefits, economic development through the provision of trained manpower, community renewal, and social control in meeting community needs (Alfred, 1980). Moreover, community colleges will be the focal point of lifelong learning and the "educational and technical bridge from the public schools to the 'world of work' and/or four-year institutions" (North Carolina Community College System, 1999, p. 14).

Community colleges may also reach individuals who may not have received computer training or computer ethics through other sources. Currently, more than 95% of all community colleges are Internet-connected (AACC, 1998). In 1994, Cross reported that community colleges have the highest number of student-owned to institutional-owned computers and the highest percentage of classes using computers for instruction. In addition, community colleges lead in the percentage of courses reporting classroom computer use. Community colleges use computer-based labs in nearly twice as many courses as public universities (Green, 1994). Bill Gates, CEO of Microsoft said:

> America is leading the way in high technology, and in the next seven years, it's estimated that 80 percent of new jobs in this country will be in high tech. Community colleges have an important role to play in making certain we have skilled workers ready to help businesses take advantage of all the opportunities in the Digital Age. (AACC, 1998)

An additional consideration involves the community colleges' opportunity to reach business and industry. Community colleges will be the primary deliverers of instruction for the work force (North Carolina Community College System, 1999). Ninety-five percent of businesses and organizations who use them would recommend community college workforce education and training programs (AACC, 1998).

The community college is also more reflective of the community it serves and has the ability to be more adaptive to the needs of the people.

> The real strength of the community college lies with the people it serves. More diverse than any other clientele in post-secondary education, those who are served by this institution reflect divergent characteristics from a broad range of society and mirror the community in which each college is located. (Palinchak, 1973, p. 251)

It is predicted that community colleges will be better able to respond to the changing demands of information technology than other educational institutions. The reasons include: growing competition from the private sector, growth of nontraditional delivery integrated with traditional campus-based programs, and the changing role of the teacher from dispenser of knowledge to facilitator of learning. In addition, "just-in-time learning" and "just-in-time training" will increase and change expectations. Finally, community colleges are expected to assume a leadership role in managing the effects of societal changes due to their relationship and role within the community (North Carolina

Community College System, 1999).

The need for computer ethics policies and ethical instruction may be more critical at the community college level as compared to other institutions of higher education. The age of the typical community college student is older than students at the university level. For many of these adults computers were not used or readily available when they attended public school. In fact, many adults enter the community college for the purpose of learning about information technology to enhance their employment opportunities.

A second group found only at the community college level is the GED and adult high school student. These individuals stop attending public school for a number of reasons. In many cases, these students are considered high risk, lacking adequate guidance and supervision. As a result, the need for ethical instruction and support may be greater for this group as compared to most teenagers their age.

The community college also has an opportunity to reach individuals who may not decide to attend an institution of higher education. Many businesses and industries provide training to their employees through community college continuing education programs. These individuals may encounter ethical dilemmas and situations more often than others, and would normally not be a candidate to receive much in the form of ethical instruction and support.

Finally, the community college reflects the community it serves. This may include ethical instruction for unemployed persons, migrant workers, and senior citizens. Thus, the community college has an opportunity to reach diverse groups of people needing computer ethics instruction who may be beyond the reach of other institutions.

North Carolina Community College System

The North Carolina Community College System may typify the need for computer ethics policies or better ones for community colleges and appears to have unique opportunities and implications for addressing organizational leadership issues. The North Carolina Community College System appears to be very representative of national statistics concerning community college systems. This state system is comparable to others in all criteria: diverse student population, high enrollment numbers, societal impact, emphasis on business and industry, and reflection of the community it serves. A second factor, which suggests that the North Carolina system may play a symbolic role for other community colleges, is their commitment to respond to the changing demands of information technology. The resulting issues and concerns appear representative of similar college systems throughout the country.

Although educational leaders within the North Carolina Community College System typically have not developed comprehensive computer ethics policies nor developed any policies at all, at least the need for guidelines for all state employees has been addressed. The Information Resource Management Division (IRMC), in conjunction with the State Information Processing Services of North Carolina, has developed a policy regarding the use of the North Carolina Integrated Information Network (NCIIN) and the Internet by state employees.

The policy entitled "Use of The North Carolina Integrated Information Network and the Internet" was created due to a perceived need for heightened awareness among public employees regarding ethical behavior concerning information dissemination and access. The policy addresses such issues as illegal or obscene usage, personal use, e-mail, accuracy of information, viruses, and software copyright and licensing laws.

While the policy provided by the IRMC does offer ethical guidance concerning appropriate use of the NCIIN and the Internet, there are limitations. This policy applies to all "government agencies" and "public staffs" under the authority of the IRMC, but does not directly address the student population within the community college system. The policy, while written for state agencies, does not consider the unique needs of educational leaders within the community college environment. Furthermore, in many cases, dissemination, implementation, and understanding of the policy have failed to filter down to those individuals governing the computer systems and labs.

Purpose of Study

Based upon the prominence of information technology, particularly on college campuses, educational leaders are being faced with ethical dilemmas that demand solutions. With these new challenges, educators need to understand clearly and be equipped to handle issues and concerns as they arise. They need to develop ethical polices, procedures, and instructions that will work. In view of this, there is a demand for scholarly research on computer ethics issues/policies in the college or university context.

Research is needed to help determine what educational leaders think about current problems and issues as well as viable solutions. There is a need for not only new research into the problem, but, given that most policies are fixed rules or codes that seem to be ineffective, there is a need to view and develop these policies using new theoretical perspectives. In addition to policies, implementation guidelines must be developed to assist educators in the provision of ethical instruction. Finally, research is imperative for closer scrutiny of the underlying principles and theoretical concepts that promote and facilitate ethical conduct by computer users.

The primary purpose of this study was to clarify, identify, and confirm the practical problems and concerns that are facing organizational leaders due to the prominence and use of information technology on college campuses. This particular study dealt with computer ethics issues, needs, and solutions within the community college setting and particularly within the North Carolina Community College System. The specific goal of the study was to discover, using survey research, the extent to which and how college administrators in the North Carolina Community College System have dealt with issues of computer ethics and computer ethics policies on their campuses. In addition, system administrators were asked for their response to a preliminary draft of an ethics policy and plan of action that incorporates the Theory of Deindividuation. The theory was used as a theoretical framework through which to explore these computer ethics issues with educational leaders, determine the underlying assumptions of computer users, and develop a model computer ethics policy and procedures that will promote and encourage ethical behavior by computer users.

Through the application of the results of a survey of 58 administrators, additional research information taken from prior computer ethics studies, and analysis of successful computer ethics policies of other educational institutions, a model computer ethics policy and implementation plan that includes ethical instruction was developed. While the policy and instructional plan are particularly applicable for the North Carolina Community College System, many of its components are applicable to other institutions of higher education as well.

A number of fundamental, practical, and theoretical questions were addressed through this study. Among the practical research questions examined in this exploratory study were: What unethical or antisocial incidents are occurring in computer labs or elsewhere on the campuses of community colleges within the North Carolina Community College System? What steps or precautions have been taken to resolve ethical problems? How effective have these measures been? Do system administrators feel that computer technology-related ethical issues have increased on their campuses and if so, why? How many community colleges within the system have a computer ethics policy at the current time? What are limiting factors contributing to a lack of computer ethics policies at some colleges? How do community college administrators believe a computer ethics policy should be aligned with the mission and purpose of higher education or the particular mission of their educational institution? What do they consider the best ways to communicate a computer ethics policy and encourage computer users to believe in it? Finally, in what ways would they enforce a computer policy, and should this apply equally to students, faculty, and staff?

At the same time, this study explored a number of theoretical questions focusing upon the Theory of Deindividuation, including: Does the Theory of Deindividuation help explain the current ethical thinking and behavior of current users of computer technologies on particular community college campuses? Is the Theory of Deindividuation a useful perspective to have when developing computer ethics policies, procedures, and accompanying instruction? Can elements of the Theory of Deindividuation be embedded in the computer policies, procedures, and instruction themselves? It was hoped that answers to these questions would lead not only to a better understanding of the computer-related ethical issues confronting community college leaders, but would also result in a model computer ethics policy and ethical instruction plan that they would be able to adopt and find effective.

Scope and Importance of Study

The scope of this study was limited to the North Carolina Community College System. This is based upon the unique needs of the system and the perceived need for a computer ethics policy to help guide organizational leaders in making the wisest decisions concerning ethical dilemmas. While this study focused upon the North Carolina Community College System, results of this study are certainly applicable to community colleges in other states and to other types of institutions of higher education within as well as outside the state.

Due to the prominence of computers on college campuses, organizational leaders have raised questions concerning effective methods for handling information technology concerns. The importance of this study is based upon the premise that the information it will provide may assist in meeting some of the practical needs of educational leaders who are increasingly faced with having to address these questions. The study also should bring much greater clarity to underlying problems in both the computer ethics area generally and in the college computer ethics context particularly.

It also is speculated that organizational leaders will increasingly find it necessary to have a policy to provide guidelines, set rules of prosocial conduct, and encourage ethical behavior by all computer users whether faculty, student, staff, or administrative personnel. Evidence provided by this study will indicate the need for and benefits of creating and implementing a computer ethics policy or a more effective policy. A model policy and ethical instruction based on a more comprehensive understanding of the ethical issues and problems and rooted in significant behavioral assumptions, could be a practical solution for those educational leaders searching for one.

In addition, the results of this study should contribute to scholars' understanding of computer technology ethics within current educational settings. It should raise new questions about computer ethics that scholars can pursue. The results of this study may also provide scholars with new insights regarding the Theory of Deindividuation and its practical applications, particularly to the computer ethics area in contemporary academic settings.

Chapter II: Review of Literature

Our information-driven society and endless quest for more knowledge has created an extensive dependency on computers and information technology. This reliance upon computers has resulted in ethical concerns and legal issues prompting organizational leaders to raise serious questions. A major contributing factor to these concerns and issues has been the use of the Internet and networking capabilities. Leaders in search of answers have received little satisfaction in resolution through governmental or legal measures.

Organizational leaders within higher education have a unique opportunity to help educate societal members and computer users to make the best moral and ethical decisions. An important component guiding and providing a foundation for ethical education of computer use is through computer ethics policies. In consideration of developing computer ethics policies, behavioral models may assist educators by providing understanding and insight concerning the underlying factors involved in unethical behavior.

To clarify, identify, and confirm the fundamental and theoretical challenges and concerns facing organizational leaders within higher education, a review of the literature concentrating on identified key areas was necessary. The literature examined here first documents the extent of the ethical impact and societal influence of computers. Literature dealing with ethics, particularly how ethics relates to computers, research showing the legal issues surrounding information technology, and studies showing the development of computer ethics as a better response to ethical dilemmas are all reviewed.

The review of literature provides insights from the business community and then turns to studies showing the effectiveness of ethical instruction within institutions of education with a particular emphasis on the effectiveness of computer ethics policies. As a final area worthy of review, behavioral models are examined for insight concerning computer behavior and related computer ethics policies.

Computers and Their Ethical Impact on Society

Confirmed in the examination of literature, similar to other technological inventions throughout history, information technology tends to have both positive and negative effects on society, and tends to raise moral and ethical concerns (Fodor 1996; Johnson, 1991; Sivin & Bialo, 1992). As early as 1969, Weizenbaum (1969) compared computers to prior electronic technology. The inherent danger, Weizenbaum (1969) noted, involves the time lag between introduction of new technology and attention to ethical implications.

Television has had an enormous and irreversible effect on our lives; computers are having a comparable impact. It has been well-documented that television had and still has the potential to impact individuals, groups, audiences, and entire cultures positively and negatively; however, television practitioners, scholars, and critics underestimated its dangers. While the impact of television has been great, computers have the potential on a unit-by-unit basis to have a far greater impact on more people's lives and more aspects of their lives. "While one [emphasis added] television set can influence one or two willing individuals, one [emphasis added] computer with a modem has the potential to affect millions of mostly innocent and unsuspecting people" (Kizza, 1996, p. 45). Computers, particularly since the growth of the Internet, have in various ways empowered individuals and made it possible for them to be mass communicators.

An even greater contrast between the computer and the television exists in the type and degree of reality they create for those who use them. Kizza (1996) suggests that computers—unlike other revolutions involving industry, automobiles and television—provide a different reality. Computers connected to a network enable a virtual societal domain, which may be defined as "boundless, colorless, cultureless, and classless" (p. 47). He concludes, therefore, that two societies exist in which protection is needed—virtual and real.

The effects of information technology parallels the impact of other revolutions. Moor (1985) equates the computer revolution with the Industrial Revolution citing two distinct stages involving technological introduction and technological permeation. During the latter stage, society has dramatically transformed computer technology to become an "integral" part of all institutions.

Lacey (1986) suggests new technological revolutions proceed through three phases. Initially, the technology is available only to a select few members of society who dominate the field. During the second phase, technology spreads to others, and finally progresses to the extent that the technology becomes so common that to do without it puts one at a disadvantage. Kizza (1996) also sees revolutions as having three stages beginning with amazement, then prosperity, and concluding with social upheaval. It is his contention that we are entering the social upheaval stage with regard to the impact of computers (Kizza, 1996).

Those who seek to understand these changes are increasingly realizing that information technology not only has already influenced lives profoundly but also will continue to do so in even greater and more diverse ways. Also necessary is an understanding that the consequences of this technology can be both positive and negative and raise ethical issues and concerns. Finally, responsible citizens must have an interest in contributing to discussions and policy-making so the advances in computer technology will not compromise human values (Moor, 1996, p. 265). Realizing the need for better understanding of the implications of information technology, the review of literature turns to ethical perspectives.

Fundamental Ethical Perspectives

As discussed earlier, there is a connection between new technology and ethical and moral concerns. Our utilization and our dependence upon information technology have penetrated all of society causing new ethical questions to emerge. Prior to further examining ethical questions related to computer technologies and their use, a basic understanding of what ethics encompasses may be helpful. Many theories and perspectives of ethics have been developed and debated for many years. Literature reflecting this is abundant and provides rich insight into what underlying ethical foundations may explain people's current behavior with regard to computer use, and what ethical views or systems might be best suited in response to ethical dilemmas attributable to information technology.

Philosophical perspectives. Ethics focuses upon and is critical in the decision-making process and actions of free human beings functioning within society. "When faced with alternative courses of action or alternative goals to pursue, ethics helps us to make the correct decision" (Laudon, 1995, p. 34).

The common perception is that ethics is relative. Negative and positive claims of ethical relativism state there are no universal moral rights and wrongs; morality, rather, is relative to one's society (Johnson, 1994). The utilitarianism theory of ethics is a form of consequentialism. Behavior is evaluated in terms of its consequences putting emphasis on "happiness-producing" consequences. The basic principle is "everyone ought to act so as to bring about the greatest amount of happiness for the greatest number of people" (Johnson, 1994, p. 24).

Deontological theories put the emphasis on internal character of the act itself. What makes an action right or wrong is the principle inherent in the action (Johnson, 1994). In essence, this suggests that individuals decide what is right or wrong based upon their internal motivation to perform a certain act. Vitell and Davis (1990) take the deontological concept one step further to categorize ethical perspectives as being deontological or teleological. The deontological view focuses on actions or behaviors of the individual, while teleological focuses on consequences.

Ethicists in general tend to differ on the locus of moral authority. Some insist that it is within the individual, while others believe it is located in larger collectives. Laudon (1995) proposes that ethical thought be arranged with two dimensions: rules versus consequences, and collective versus individual. This results in four "schools" of ethical thinking. School one includes the collective rule-based ethics that suggest we should follow rules of ethics that are derived from the logic of the situation. School two states that individuals learn what is right by looking inward to universal and timeless rules derived from religious beliefs, institution-derived definitions of "rightness," and self-analysis. The third school of thought suggests individuals should look in the real world to discover empirically what is right and wrong. The final school of ethical thinking assumes that each individual serves social welfare best through analysis and experience discovering one's self-interest and pursuing that interest to the full (Laudon, 1995).

The various ethical views and schools of thought contribute to a more extensive understanding of ethics. As a result, this may enable educators to embrace the diversity found within individual, as well as societal, interpretations of what constitutes ethics when developing computer polices and ethical instructions.

Perspectives on computer ethics. The discussion now turns to how ethical concepts are being impacted by computers and information technology. It is important to understand exactly how ethical distinctions and guidelines are being challenged and what concerns are being raised due to the impact of information technology.

Rubin (1996) suggests that information technology creates seven temptations for individuals. The first of these is the temptation for speed in gathering and transmitting information, which is increased through the computer. The second temptation concerns privacy and anonymity. This temptation permits unethical actions to be performed in absolute or near-absolute privacy in one's own home. This temptation also increases moral distancing and remoteness of the act itself.

Temptation three, facilitated by information technology, permits individuals to steal information without actually removing it. The fourth temptation is the aesthetic attraction of computer technology. "Work with computers requires creativity, inventiveness and artistry in the solution of technological problems" (Rubin, 1996, p. 129). The next temptation is the increased availability of potential victims; computers provide the opportunity to be unethical toward thousands of people with very little effort. Temptation six focuses on an international scope suggesting that the geographical reach of information technologies has few limits. The final temptation involves the potentially enormous power and destructive capacity of information technologies.

To rephrase the temptations, the fact that computer technology allows one privacy and anonymity creates an environment conducive to individuals being tempted to perform destructive actions toward unlimited numbers of individuals with great speed, power, and control. The capabilities and temptations being provided by information technology have led to many ethical questions and concerns. Latimore (1997) poses an intriguing question, if one becomes invisible—why should one act justly? Rubin (1996) asks, "If we can do something so quickly, aren't we more likely to presume that in many instances, the chance of being caught is very small?" (p. 127).

A potentially greater concern, "Certain characteristics of information technologies promote a moral distancing on the part of the individual as an ethical agent; that these technologies allow the agent to create a moral distance between the act and moral responsibility for this act" (Rubin, 1996; Friedman, 1990). Stephen Brockmann states that when other individuals are simply blips on the computer screen, they become dehumanized. It is no longer a moral crime to kill them, since the Fifth Commandment does not extend to computer blips. In fact, "People seem naturally predisposed to depersonalize complex systems, and computers permit new opportunities to perform unethical activities" (Neumann, 1991, p. 106).

Moral distancing also has the effect of creating an "invisibility factor." While some crimes remain crimes regardless of the means used to perform them, difficulty arises when individuals associate criminal actions with physical evidence of destruction. Computers operate with software and instructional codes not visible to the user, and many victims of computer crime are represented only through the software rather than in a physical realm. Without the physical nature of technology, the offense does not seem so bad (Friedman, 1990).

Anderson (1996) believes that most people caught misusing computers do not even consider their "crime" to be unethical or dishonest. In a sense, computers have "de-personalized" crime and made it appear victimless (Anderson, 1996; DeMaio, 1990, 1991). Sivin and Bialo (1992) lend further support by stating that most individuals have a good sense of right and wrong concerning physical property, yet view nonprint information quite differently.

Alexander (1989) quotes Larry Potts, chief of the white-collar crimes program at the FBI, as saying that too many people believe computer crimes are victimless and the illegality of accessing computer systems causes little harm. The same people who would never break in and physically enter a private database of information do the same act through the computer without compunction.

This invisibility factor also impacts ethics in another area unique to information technology. Computer operations are invisible, and while individuals may be knowledgeable about inputs and outputs, they are barely aware of internal processing. Moor (1985) suggests the ethical significance of invisibility is "invisible abuse." He defines this as "intentional use of the invisible operations of a computer to engage in unethical conduct" (Moor, 1985, p. 273). Invisible abuse can include invasion of property as well as invasion of the privacy of others.

To further complicate ethical dilemmas, while some computer concepts may appear invisible, others may in fact emerge from "invisible" programming to create the illusion of reality. The computer can simulate real or imaginary phenomena and is capable of creating a “virtual” world or virtual reality. Some virtual realities are easy to recognize while others are much more sophisticated and difficult to distinguish from the real world. Even more dangerous, virtual reality can exist as a world entirely inconsistent with ours (Fodor, 1996, p. 261).

Fodor (1996, p. 260) states that virtual reality makes it necessary to re-examine human behavior and the viability of our ethical systems. This is due to the premise that virtual reality alters concepts of right and wrong causing actions based on these values to change as well (Fodor, 1996, p. 261).

Computers and information technology continue to have a profound impact on individual perceptions of prosocial behavior and ethical conduct. Information technology enables computer users to perform unprecedented activities that many do not perceive as unethical.

Computer ethics versus computer laws. While information technology is impacting ethical perspectives and societal norms, many educators are seeking thoughtful answers. Is the solution to ethical dilemmas new computer laws, or is it computer ethics? Which may be more effective and realistic? More importantly, which may actually change behavior? If we are hoping to facilitate prosocial behavior and are interested in the best interests of society as a whole, then we must examine the evidence.

Computers have provided the ability to connect with others in a networked society, greatly altering our culture. Members of networked communities engage in social behavior. This social behavior consists of values, or general statements about the “desirable”; behavioral norms, including etiquette and convention; and beliefs that provide history and world view (Denning & Lin, 1994).

In light of the fact that social behavior may be more extreme on electronic networks, effective ways to regulate and promote ethical behavior become essential. Society attempts to regulate human behavior based upon cultural values, norms, and beliefs. When regulation of behavior fails to be influenced by friendly persuasion, parental admonition, social pressure, contracts, licenses, or informal agreements, legal remedies are soon sought in settlement of disputes. The law and coercive power of the state to enforce laws tend to be the mechanism invoked by society to shape behavior only after all other avenues have been exhausted and found not effective (Denning & Lin, 1994).

Sullivan (1996) states,

> The reduction of computer ethics to computer law is not uncommon, and usually takes the form of saying that whatever is not illegal is not unethical and, in some cases, even morally required. The reduction of ethics to law underestimates the range of ethics, the function of law and the relationship between the two. (Sullivan, 1996, p. 293)

The social effects of computing may be viewed as a "classic problem of balancing the freedom, needs, and interests of some individuals against the freedom, needs, and interests of others" (Johnson, 1994, p. 107).

The social implications of computing also revolve around two critical values—autonomy and access. It is counter to the value of individuals when autonomy of some is increased or improved at expense of autonomy of others. A just society exists when freedoms and constraints are fairly distributed and individuals have access to opportunities to achieve their ends (Johnson, 1994).

While an ethical response to technology-induced concerns and issues appears a more viable solution than increased legislation; nevertheless, the legislative arm of our government has been forced to examine the impact more closely. The courts have been mixed in their responses to the jurisdictional issues created by information technology.

Legal Issues

The review of existing documentation indicates that legislative issues are receiving unprecedented attention resulting from the impact of computers. Such issues as privacy, freedom of speech, and copyright concerns, while existing previously, have had to be re-visited, and in some cases, modified to accommodate the new technological platform.

Anderson (1996) insists that current laws are outdated and confusing because they were not written for technologies of today. The most frequently discussed legal topics are user privacy, freedom of expression, and intellectual property rights (Petersen & Hodges, 1997). Others add access and accuracy to the list of serious legal issues (Connolly, 1997; Mason, 1986). Palmiter (1996) suggests that ethical issues may all be reduced to one—responsibility.

Privacy. Privacy may be defined as the claim of individuals to determine for themselves when, to whom, and to what extent individually identified data about them is communicated or used (Cooley, 1990). Johnson (1994) states that friendship, intimacy, and trust cannot develop without privacy, which is also necessary for autonomy.

Many people incorrectly assume there is a right to privacy in the Bill of Rights within the United States Constitution. Although the US Constitution does not provide the right to privacy, the Fourth Amendment does protect against "unreasonable searches and seizures" by the federal government (Petersen & Hodges, 1997). However, some protection of privacy is afforded in selected state constitutions and state privacy laws.

Two forces threaten privacy: one is the growth of information, and the second is the increased value of information in decision-making (Mason, 1986). Greenberg (1986) states that computer technology is well on its way to obliterating privacy in numerous facets of our lives with potentially no end. Anderson (1996) adds that so much information is available to Internet users that the value of private, secure information is being lost.

The Internet is contributing to the legal ramifications of privacy issues by allowing unprecedented invasions of personal privacy. A survey of Internet users by Atlanta-based Georgia Institute of Technology in 1997 found that privacy was the most important issue concerning the American public. Thirty percent of those surveyed said it was their greatest concern about the Internet. A Business Week/Harris poll found two thirds of those surveyed would use the Internet for business purposes if they felt privacy was protected (McAllester, 1998).

The law distinguishes among four forms of invasion of privacy: a) intrusion, b) disclosure of confidential information, c) publicly characterizing someone in a false or misleading manner, and d) appropriating someone else's name or likeness for one's own benefit. Intrusion is easily accomplished due to the ability of computers to provide anonymity and to provide unauthorized access for hackers. The anonymity factor may cause difficulty in developing a trusting relationship, in some cases, with those with whom information is shared (Connolly, 1997).

Disclosure of confidential information becomes much easier through information technology. Collections of information reveal intimate details about a person and can, thereby, deprive an individual of the opportunity to form certain desired professional and personal relationships.

The computer also enables small pieces of information to be linked forming a composite picture of an individual. Mason (1986) suggests that "computer matching and integration of data files into a central databank have enormous ethical implications" (p. 7). Prior to computers, hard copies of files were stored in cabinets that limited the amount of data and how it could be accessed or retained. Electronic records do not have these limitations. Information can be combined and compiled to produce a profile of an individual. This individual profile may also be easy to copy and distribute, and there is always the possibility that some of the data may be in error (Johnson, 1994).

Stealing an individual's identity and using it for financial gain on the Internet is increasingly common. Cases investigated by the Secret Service estimate that individual and institution identity theft costs rose from $450 million in 1996 to $745 million in 1997 (McAllester, 1998). An important aspect of computer-based data is the ease with which computer-based data files can be stripped of identifying information, thus making it easy to use another's name for one's own benefit (Cooley, 1990).

The Privacy Act of 1974 was the first effort to contain threats to privacy created by technological advancements (Cooley, 1990). However, most lawmakers feel the Internet develops too quickly for static laws to work effectively. Politicians encourage the Internet industry to regulate itself. Recently, under pressure from governmental administration and the Federal Trade Commission, more than 50 Internet companies formed the On-line Privacy Alliance, a group dedicated to developing a set of self-regulatory privacy guidelines (McAllester, 1998).

Freedom of speech (censorship). Public institutions are subject to the First

Amendment providing freedom of speech. Some groups argue that the Internet is a public forum and is protected by the First Amendment. As such, they state that governmental institutions must have a "hands off" approach.

Much adult material is protected by the free speech clause of the First Amendment. "Indecent" material is included in that protection, although most states have prohibited the sale and distribution of it to minors. In spite of this, the American Libraries Association holds that minors have the right to be provided with anything, including pornography, in a public library at the taxpayers' expense (Tweet, 1998).

There is a fine line between material that is considered indecent and material that is considered obscene. While indecent material is interpreted to be covered by the free speech clause of the First Amendment, obscene material is not afforded such protection. To be classified as obscene, material must meet all of the following criteria: first, would the average person, applying contemporary community standards find the work, taken as a whole, appealing to prurient interests; second, does the work depict or describe, in a patently offensive way, sexual conduct specifically defined in applicable state law; finally, does the work, taken as a whole, lack serious literary, artistic, political, or scientific value.

Ethical issues involving the Internet are abundant, and attempts to regulate it have failed, being referred to as censorship. Johnson (1995) suggests that the content of the Internet is neither regulated nor moderated. The presence of potentially objectionable materials on the Internet, she argues, cannot become justification for denying rights to the information.

The National Education Association (NEA) represents 2.3 million teachers and other employees in America's public school system. They addressed indecency on the Internet to the US Senate Committee on Commerce, Science, and Transportation on February 10, 1998. The NEA stated that student exposure to indecent material on the Internet demands attention. The Internet is a powerful and useful tool, yet there must be a balance between encouraging student responsibility, discernment, and critical thinking skills while shielding these students from material deemed inappropriate or indecent (Congressional Testimony, 2-10-1998).

Attesting to the effectiveness of shielding, CompuServe, an Internet service provider, blocked international customer access to 200 sexually explicit sites causing angry protests from its customers. Some referred to it as an attempt to filter out some objectionable material and felt that it would lead to broader censorship (Benkelman, 1995). CompuServe explained that the German government had demanded it delete member access to the newsgroups. Benkelman (1995) quotes Nicholas Negroponte, director of Media Lab at Massachusetts Institute of Technology and author of "Being Digital," as observing that governments do not understand that the Internet cannot be controlled and is unstoppable (Benkelman, 1995).

Sowell (1997) brings up a significant point when he states that people can be sued for slander and libel, but on the computer, free speech is given such an extreme interpretation that our children's welfare is not considered important. He goes on to suggest that if we are serious about our children, then we should not let anyone prevent us from protecting them by using the word "censorship."

We have evolved an ironic scenario within our society. An organization may be held legally responsible for messages created and distributed by employees. In many cases, e-mails can be identified with the company for which an employee works regardless of where the message originates. Nevertheless, if a company or institution monitors electronic communications in an effort to catch offensive language, they have actually increased their liability for content of every message originating from the system. The company's system can be seen as acting as a publisher in this type of case.

Recently, Prodigy was named in a $200 million lawsuit for comments one of its users made. Prodigy did not originate the message but was the mechanism by which it was distributed (Slater, 1994). Companies, it has been decreed, may be provided some protection by not regulating content, being held as a distributor rather than a publisher (Stratton Oakmont and Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, S.D.N.Y., 1991).

Intellectual property (copyright issues). The biggest threat to copyright is the ease with which material can be copied and distributed. This makes information hard to safeguard because, unlike tangible property, it becomes communicable and hard to keep to oneself.

Contrary to popular belief, no formal notice or registration is necessary for work to be protected under copyright law. Registration is required only prior to bringing lawsuit. Copyright law provides the owner with the exclusive right to reproduce or copy material, prepare derivative works, distribute it by sale or transfer, and perform or display it in public (Petersen & Hodges, 1997). The much-used "fair use" provision of the Copyright Act has four factors. Fair use is dependent upon the purpose of use (non-profit educational purposes), the nature of the copyrighted work, the amount and proportion of whole copyrighted work used, and the effect on the copyrighted work's market potential or value (US Congress, Office of Technology Assessment, 1986).

In an ethics survey conducted in the early 1990s, Computerworld found that 62% of the respondents felt they should be able to download and share materials without violating copyright law. There was the perception that the material viewed through the computer was similar to television and free for all to view. Although 78% of the respondents agreed that it should never be done, 47% admitted to copying commercial software. Another finding indicated that individuals understand and respect privacy when violations harm an identifiable person, but rationalize that making copies of PC software packages has little effect on giant vendor companies led by millionaires (Betts, 1995).

In a recent case, the Los Angeles Times and Washington Post jointly filed a copyright-infringement suit to bar a Web site from copying and posting stories from their newspapers. Jim Robinson, whom they were suing, had been invited by the papers to link to their site rather than copy materials. Robinson insisted that the First Amendment and the "fair use" doctrine of copyright law protected his activities (Miller, 1998).

Connolly (1995) states that freedom does not mean license and reasons that unauthorized copying of software is illegal, unethical, and not in one's self-interest. It is illegal to make copies other than an archival copy, and it is unethical to take something belonging to another without permission. Furthermore, such action is not in one's self-interest because creators will either increase prices to cover costs of theft or reduce creations due to lack of profitability (Connolly, 1995).

Legislative attempts to regulate the Internet. In order to protect children, the Telecommunications Act of 1996 included a provision called the Communications

Decency Act. Exxon-Coats Communications Decency Act states that current obscenity laws apply to computers. It protects users from on-line harassment and prohibits use of a computer to lure children into illegal sexual activity. The CDA also provides for compliance through good-faith use of reasonable, effective, and appropriate means to restrict children's access to indecent or pornographic material. Penalties are imposed on people who transmit pornographic material via computer networks accessible to children (Computerworld, 1996).

President Clinton signed the Act into law on February 8, 1996. The American Civil Liberties Union and 19 other organizations filed suit challenging its constitutionality, and it was struck down by the Supreme Court in 1997 (Petersen & Hodges, 1997). This was the court's first effort to extend First Amendment principles into cyberspace. Justice John Paul Stevens held that speech on the Internet is entitled to the highest level of First Amendment protection, similar to that given books and newspapers. This interpretation stands in contrast to more limited First Amendment rights accorded to speech on broadcast and cable television, where the court has tolerated a wide array of government regulations.

The Communications Decency Act failed for a number of reasons. It was too broadly stated, and the community standards test is not applicable when using the Internet which has no boundaries (Connolly, 1997). University of Florida professors say it may never be possible to regulate the Internet because it is so massive. In addition, the government would experience difficulty in restricting material from the Internet because the Internet has not been classified as a certain type of medium. This appears to be the basis of the difficulty of applying broadcast media "indecency" standards to computer networks (Vieira, 1998).

The Child Pornography Prevention Act of 1995 makes it a criminal act to produce and distribute material that depicts children engaging in sexually explicit conduct, whether or not the material was produced with children or entirely by a computer. In September 1996, a bill introduced by Senator Orrin G. Hatch making it illegal to produce "morphed" child pornography passed in Congress. Morphing is achieved by taking innocent pictures of children and altering them by computer. The child's head is then grafted onto the body of a nude slender adult who is shown engaged in sex acts.

Because pedophiles use images to convince children that sex with adults is enjoyable and natural, mental health professionals worry about the long-term impact of child pornography on the Internet. Child pornography on the Internet tends to legitimize all types of sexual conduct, which is dangerous. Trebilcock (1997) also notes the danger of "virtual validation," the networking of pedophiles able to contact others with similar beliefs through the computer. An example is the Orchid Club, the first known example of pedophiles using the Internet to show the actual sexual torture of a child.

In 1998, Senators John McCain (R-Arizona) and Ernest Hollings (D-SC) introduced legislation known as the Internet School Filtering Act, requiring schools and libraries to block "explicit" material on the Internet or lose federal funding from the universal service program. Their bill requires schools receiving universal service discounts to certify with the Federal Communications Commission (FCC) that they are using a filtering or blocking system on computers. Libraries must have one or more computers suitable for minors' use.

The universal service program came out of the Telecommunications Act of 1996, which directed the FCC to develop a plan for universal service to consumers and schools. The required prevention is not censoring, it is assumed, but rather filtering what comes out of computers. Allowing different communities to set standards and requiring only one computer in each library to include the filtering software may be a responsible way around the constitutional issues of banning free speech. The American Civil Liberties Union still considers this legislation unconstitutional (Pietrucha, 1998).

This legislation is designed to protect children from exposure to sexually explicit and other harmful material when they access the Internet in school or a school library. McCain stated, "If schools and libraries accept these federally-provided subsidies for Internet access, they have an absolute responsibility to their communities to assure that children are protected from on-line content that can harm them" (Press Release, 1998).

A federal judge struck down a Virginia law barring state employees from viewing sexually explicit communications on-line, terming it "unconstitutional." The American Civil Liberties Union filed that suit on behalf of six professors from Virginia Commonwealth University, George Mason University, Blue Ridge Community College, Old Dominion University, and the College of William and Mary. The professors argued that the law made it impossible for them to use the Internet productively for researching academic disciplines. Professors, it was pointed out, had to obtain written permission to receive or send materials to which their students had free access (Pietrucha, 1998).

In light of the lack of success with legislative attempts and in view of the inherent limitations of law, the computer law versus computer ethics debate appears to confirm that ethics, in this case, may serve society more effectively than law.

Development of the Computer Ethics Field

The existing body of literature indicates that a more promising response to the technology-driven ethical concerns is through the application of computer ethics instruction. There is an increasing demand for developing computer ethics as a field worthy of further research. As a result, computer ethics is becoming a field in need of research based upon a necessity to provide information for educational leaders.

The legal structure appears to be limited in its ability to facilitate ethical behavior effectively. The law, by its nature, cannot be expected to provide adequate guidelines for behavior in an evolving environment. A sense of personal responsibility is difficult to develop in electronic networks due to the conflict in understandable desires to both authenticate and conceal identities. Moreover, to be effective, new legislation requires a social consensus about what is new and unique concerning technology as compared to other media as well as what values that legislation will embody. Such a consensus does not exist today (Denning & Lin, 1994).

The third limitation of existing laws focuses on expectations of the legal system for individual behavior. It is generally agreed that members of society behave in a rational and respectful manner in dealings with each other regarding proprietary interests. The limitations in existing laws are due to the ease and ability to replicate, alter, and manipulate images and text (Denning & Lin, 1994).

History, definition, and contributors. Walter Maner introduced the concept of computer ethics in 1976. Maner's formalization was based primarily on the work of Donn Parker, a researcher at SRI International and author of the first code of ethics for the ACM. Maner noticed that when computers are involved in ethical problems, they often exacerbate the moral issues, and, in certain cases, they can create new moral dilemmas.

Parker, Swope, and Baker (1990) suggest that the application of ethics in information sciences is more difficult than in other disciplines. Computer and data communications alter relationships among people; information in an electronic, magnetic form is more fragile than comparable information on paper. In addition, business transactions rely on handwritten signatures while electronic transactions do not. Furthermore, unlike computer science, some professions have had hundreds of years to develop appropriate ethical concepts.

Other computer ethics contributors in the late 1970s and early 1980s include Jim Moor, John Snapper, and Lance Hoffman. Moor (1985) defines computer ethics as the "analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology" (p. 266). Computer technology provides new possibilities for acting, thus new values emerge. Computer ethics is a dynamic and complex study, which considers relationships among facts, conceptualizations, policies and values.

In 1985, Deborah Johnson published the first book on the subject entitled Computer Ethics. She explores the idea that computers create complexity due to the fact that it has not been clear what software is. Are software and computer programs products or services? Different laws apply to each. She summarizes in a later publication, "The study of computer ethics turns out to be the study of human beings and society—our goals and values, our norms of behavior, the ways we organize ourselves and assign rights and responsibilities, and so on" (Johnson, 1994, p. 6).

Researchers in other disciplines have also examined computer ethics. Judy Perrolle has written from a sociological discipline; Sherry Turkle, from a psychological perspective; Keith Miller and Don Gotterbarn, from the perspective of computer science; and Michael Gemignani, from the discipline of law (Fodor, 1996).

Gotterbarn (1998) believes there is very little progress in the field of computer ethics contributing toward a unified concept. There is, he argues, an absence of a "coherent concept of computer ethics." Unethical acts simplified by the existence of a computer do not automatically make the act an issue in computer ethics. The computer has become a way of life and has impacted nearly every dimension of life, and the absence of a clear concept of computer ethics allows all sorts of interesting moral dilemmas to become "ethical" issues.

The scope of computer ethics has been made so broad that it includes numerous and conflicting values and methodologies. Unlike medical ethics, most of the discussions in computer ethics are about things beyond the control of the individual professional. The only way to make sense of computer ethics is to narrow its focus to those actions within control of individual moral computer professionals (Gotterbarn, 1998).

Professional codes of ethics/standards. As noted above, computer-related legislation started to appear in the late 1970s—although the need for ethical behavior was recognized in the late 1960s. Three of the prominent professional societies for computer science professionals have adopted codes of ethics, standards, and professional behavior. These are the Association for Computing Machinery (ACM) which is the oldest and largest, the Institute of Electrical and Electronic Engineers (IEEE), and the Data Processing Managers Association (DPMA). Additional professional societies that have developed such codes include Canadian Information Processing Society (CIPS) and British Computer Society (BCS) (OZ, 1992).

Common ethical themes among the codes of professional societies include: a) regard for dignity and worth of other people, b) a belief in personal integrity and honesty, c) responsibility for work, d) confidentiality of information, e) regard for public safety, health and welfare, f) participation in professional societies to improve standards of the profession, and g) public knowledge and access to technology as equivalent to social power. All codes emphasize relationships and interactions with people rather than with machines (Burnett, 1996).

Johnson (1985) proposes that professional codes of ethics be examined in light of five types of obligations. These consist of obligations to society, employer, clients, colleagues, and professional organizations. Johnson and Snapper (1985) suggest five objectives that professional codes of ethics should strive to achieve. Objective one is inspiration of the members of a profession to act more ethically. The second objective is sensitivity and awareness of the moral aspects of their jobs. Others include discipline to enforce certain rules to achieve integrity, advice in cases of moral complexity and ethical dilemma, and finally, awareness and being alert regarding what to expect of members when they are performing a job (Oz, 1992).

The main focus of codes of ethics is to ensure that work has moral integrity (Summers & Markusen, 1992). Effective codes of ethics at both fundamental and procedural levels serve two complementary purposes. First, they protect consumers and society from institutionalized destructiveness by facilitating professional activities in the best interest of the public good. Second, various types of ethical guidelines protect the individual professional who is instructed by a superior to perform an unethical organizational task (Summers & Markusen, 1992).

Kizza (1996) equates computer ethics with a more universal ethical principle that stresses socialization and education rather than enforced compliance. Thus, these codes of ethics should aid in individual decision-making rather than attempt to set up specific punitive laws.

DeGeorge (1990) believes that computing professionals have a special responsibility to consider long-term effects of their actions on society and that their responsibility is greater than that of the average citizen. One factor underlying the concern about computer ethics is the lingering suspicion that computer professionals may be unprepared to deal with ethical issues that arise in the workplace (Parker, 1978). In one study, Parker (1976) found that many computer professionals failed to recognize when ethical issues were present. He hypothesized that lack of ethical emphasis in computer education and training programs could have failed to underline among professionals that certain types of unethical conduct are, in fact, criminal.

Another reason why computer ethics has become more important is due to the increased threat of collective violence. Collective violence is defined as "large-scale destruction to which many people have contributed" (Summers & Markusen, 1992, p. 92). They posit that computer professionals should be concerned about collective violence for a number of reasons. First, one area of potential abuse is in intelligence spying on individuals and computer systems. Another potential concern involves nuclear weapons.

Professionals may justify destructive work through the use of several psychological mechanisms. These include dissociation, rationalization, compartmentalization, amoral rationality, technological curiosity, and distancing effects. The probable cause of destructive professional work basically comes down to "economic practicalities." One effective means of combating collective violence is through development of a professional code of ethics balancing self-interest with the public good (Summers & Markusen, 1992).

Due to the newness of the computer ethics field, other fields may assist in the development and understanding of how ethical issues relate to information technology. As computer ethics increases in attention, and as further research is demanded, business ethics can assist in confirming major assumptions.

Business Ethics/Organizational Leadership

The existing literature confirms that the business field has not been exempt from ethical concerns prompted by information technology. Some of the basic standards they have set and their findings concerning ethical and moral issues in business provide us with some insight. In particular, they shed light on the need for computer ethics standards and what those should consist of for educational institutions.

Organizational motives to utilize information technology have resulted in ethical issues. The challenge to gain increasing competitive advantage from the use of information technology requires constant monitoring of emerging technological developments and a continuous search for problems in need of a resolution. Hammer (1993) contends that technology exploitation is a critical factor for success and must become a core competency within every competitive company.

Burnett (1996) sees information technology as a major component intertwined with the business change process. Additional organizational incentives to utilize information technology consist of cost-saving benefits, improvement of production processes, and embedding information technology into products (Jarvinen, 1992).

As a result of the legal, social, and moral implications resulting from information technology, organizations have been forced to contend with ethical behavioral issues. Morris (1996) reasons that organizations and employees have a responsibility to encourage and demand high standards of ethical behavior. Kamay and Adams (1992) warn that any organization lacking consensus on security and ethical values guiding business behavior is susceptible to creating an environment of criminal opportunity and indifference.

Perhaps part of a company's attempt to hold employees to a code of ethics is to protect the firm from a scandal resulting from legal action. An additional motive is the realization that the company is part of a larger society and should be aware of how its actions and practices affect others outside the company (Keying In, 1997).

Accountability for individuals and internal publics is also an important consideration for ethical behavior within the organization. This is based upon the premise that there is an inherent tendency for substitution of impersonal forces, primarily technology, for human agency (Laudon, 1995).

A recent survey by the American Society of Chartered Life Underwriters, Chartered Financial Consultants, and the Ethics Officer Association showed that 45% of those surveyed said they had committed about one dozen actions over the past year that are considered unethical or in a gray area. Thirteen percent of those surveyed said they had used company computers to shop the Internet. Four percent admitted to having performed actions to sabotage the system. Six percent accessed private files without permission while 13% admitted to copying company software for personal use (Jones, 1998).

In a similar study, Vitell and Davis (1990) found that 47.5% of management information system professionals believe there are many opportunities to engage in unethical behavior, while only 19.7% believe that MIS managers within their firms actually engage in unethical behaviors. A majority, 73.8% of those surveyed, believes successful MIS managers were more ethical than unsuccessful managers, and 75.4% believe one does not have to compromise one's personal ethics to be successful. In spite of top management support, only 13.1% of the respondents reported that their company had a formal, written code of ethics that guided computer behavior.

F. Stanford Wayne and Patricia Chapmen mention some common complaints against today's employees in the 1992 NBEA Yearbook chapter. The primary complaint of managers was the disregard for ethical considerations by workers. They conclude by suggesting that employees be trained to keep all types of business information confidential and to understand they are to use computer equipment, software, and materials only for business functions (Keying In, 1997).

Effective leadership appears to be a key element in reducing and controlling unethical behavior. A survey by Pitney-Bowes, in Stanford, Connecticut, found that the moral or ethical tenor of a company is established by the example of leadership (Zemke, 1977).

Hegarty and Sims (1979) examined the potential effectiveness of corporate control procedures on unethical behavior in order to provide insight about selected environment conditions and characteristics that might influence unethical behavior. Their findings indicate that unethical behavior can be strengthened or weakened by environmental conditions that surround the behavior. Thus, corporate policies and goals can be regarded as a form of stimuli having a deterring influence on unethical behavior.

In an earlier study, Hegarty and Sims (1978) found that when unethical behavior was rewarded with higher profits, such behavior occurred at a higher frequency. When the threat of punishment was present, however, there was a noticeable reduction in unethical behavior.

A study conducted in the late 1980s by Vitell and Davis (1990) noted that the existence of industry codes of ethics caused individuals to be more optimistic about a positive link between success and ethical behavior. An emphasis on ethical behaviors within one's industry and among top management helps create an environment wherein successful managers are perceived as ethical managers. A further finding indicates that if top management does not support ethical conduct, it becomes less likely that subordinates will behave ethically (Vitell & Davis, 1990).

Therefore, it seems imperative that organizations should write and enforce codes of ethics as well as provide ethical instruction. If more top managers took such a stance, this could potentially eliminate some unethical practices (Vitell & Davis, 1990). Zemke (1977) suggested earlier that senior executives should keep ethics a continuing discourse starting at the policy level.

Ravitz (1995) reasons that organizational leaders must develop their own policies and determine if existing ethical codes address the use of new information technologies. Kallman (1992) emphasizes that dealing with unethical computer use requires the same kind of management skill and attention, as does any other kind of organizational risk. As such, managing risk from unethical use is best achieved by creating organizational ethical codes and by maintaining an ethical computer environment and corporate culture which is supported by top management.

Computer Ethics in Education

The existing research and studies related to computer ethics in education provide insight and understanding concerning student perceptions, concerns of educators, effectiveness of ethical instruction, and whether a computer ethics policy and ethical instruction can, in fact, make a difference promoting ethical decisions by computer users.

Information technology is infiltrating almost every aspect of educational institutions from kindergarten to college. Much like in the business field, with a benefit such as this also come potential problems and ethical issues.

The widespread introduction of computers in educational institutions within recent years has increased student usage from 27% in 1984 to 69% in 1997 (US Department of Commerce, 1997). Additional statistics indicate the proportion of schools with Internet access has increased from 35% in 1994 to 89% in 1998 (US Department of Education Statistics, 1998).

Marvin Cetron (1988) predicted that by the year 2000, high-school seniors will come into contact with as much information in one year as did their grandparents in an entire lifetime. In his State of the Union speech in January 1996, President Clinton set a goal to connect every classroom to the Information Superhighway by the year 2000.

Hunt and Paplewis (1989) believe, "The advent of computers has had a major impact on the nation's schools" (p. 3). Anderson (1996) adds that the potential dangers in our schools are due to the fast progression of technology and the general lack of understanding surrounding what technology has created.

Student ethical perceptions. The review of research indicates the existence of conflicting views concerning the ethical perceptions of students. In 1991 and 1992, the Joseph and Edna Josephson Institute of Ethics conducted a survey of ethical attitudes and behavior of 9,000 individuals. Their findings reveal a high proportion of young adults actively struggling with their concept of ethics and behavior. They also found that a large number of high-school and college students regularly engage in dishonest and irresponsible behavior.

The researchers conclude that the problem is not that young people do not value honesty and integrity, but rather that they value other things more. A summary finding showed that college students and those out of school are more likely than high-school students to rank ethical values more highly than nonethical ones. Moreover, only the out-of-school group ranked being honest and trustworthy as a number one value (Josephson, 1992).

Roderick, Jelley, Cook, and Forcht (1991) found that 97% of the students surveyed consider themselves honest. More than one third, however, expressed a willingness to attempt an illegal act for profit in the business world if they believed their chances of getting caught were slim. In a similar study, 80% of the economics students surveyed reported observing cheating by classmates. As many as 50% admitted to cheating themselves and were more likely to cheat when they perceived others also cheating. In fact, 70% of the students considered cheating either not a problem or a trivial problem (Bunn, Caudill & Gropper, 1992).

Chaney and Simon of Memphis State University surveyed the ethical attitudes of college students and found that only 33% believe copying software for personal use is unethical. Almost half reported that they had not heard faculty speak against such practices (Day & Day, 1996).

Available research focusing on business students in particular leads to similar findings concerning ethical perceptions. In a study by DuFrene, Elliott-Howard, and Daniel (1990), a survey was administered to business faculty members, business practitioners, and students enrolled in a business course. The responses indicated that 61% of the students view themselves as being more aware of ethical concerns than prior students. In contrast, 62% of the faculty felt that present students have the same level of ethical standards as those in earlier classes. A final finding indicated that a majority in all three cohorts surveyed felt that student ethical standards were typical of those found in the business community.

Magner (1989) surveyed students from various business schools to determine their ethical perceptions. The findings showed that while 63% believe that the MBA curriculum should include a mandatory ethics course, only 26% reported that their school currently required one. As many as 97% of those surveyed agree that good ethics is good business; however, 71% believe that being ethical in business could hurt them in some instances. Fifty-six percent of the respondents felt that the business world operates on a separate ethical standard, and 22% responded that the separate standard was appropriate. Of the students with prior business experience, 60% had witnessed unethical business practices. A final finding showed that nearly all those surveyed felt employers should provide ethics training.

In a more optimistic study, attitudes of university students in Australia and the United States were surveyed concerning the teaching of business ethics. Findings from the study indicate students placed an importance on business ethics education and felt that business ethics courses are valuable. Finally, students view ethical behavior as leading to positive outcomes for the corporation (Stewart & Felicetti, 1996).

The literature reports on information system students and their perceptions of ethics. Research conducted at the University of Cape Town examined the differences between information system managers and information system students. The rationale for the comparison is the fact that information system students will become practitioners and representative of entry-level computer professionals. The findings from this study showed that students have different attitudes than those held by managers and students are more permissive in their attitude toward potentially unethical behavior. The researchers conclude that the more ethical responses by managers may result from more personal experience. This confirms that experience may have a direct impact on student attitudes (Parker, Swope & Baker, 1990; Paradice, 1990).

The purpose of the Cape Town study was to determine whether information systems students and other business administration students perceive computing ethics similarly. Fraud and hacking, software piracy, viruses, and ownership of e-mail were among the ethical issues addressed. The findings showed that information system students were somewhat more protective of those in their chosen profession than were other students. In some instances they were more forgiving, but they were also more critical of inappropriate use of software. They also tended to believe more than other business administration students that information systems personnel are justified in not following instructions from supervisors when consciences dictated otherwise (Ownby & Moses, 1994).

Another study comparing information system students and business administration students found that both groups had similar ethical perceptions, yet they were different from the ethical perceptions of executives. Slater (1991) found that of the 300 James Madison University students surveyed, the majority appeared to worry less than executives about computing ethics, and more than half of the students admitted to using computers for unethical means.

An examination of social forces and contributing factors may enable a more comprehensive understanding of how student ethical perceptions are formed. A qualitative study by Friedman (1990) examined how societal forces, concerning largely comparable issues of computer property and privacy, affect school practices and resulting student perceptions. He found that teachers were inconsistent in condoning and condemning the copying of commercial software and the use of unauthorized copies. The conflicting classroom practices occurred because teachers were in an ethical dilemma. Funding limitations forced them to make a choice between compromising the students' education or upholding the law. While using illegal copies was a poor model to students, refraining from such use meant not offering needed computer courses.

Friedman (1990) also found that both teachers and students had little concern for the privacy of classroom computer files in light of the need for sharing and collaborative learning. The results from this study indicate societal forces have power to constrain school practices particularly in instances where these affect individuals beyond the school community. Organization of the school computer privacy practices was left within the jurisdiction of the school and subordinated to educational goals. In contrast, computer property, copying commercial software at school, affected individuals beyond school. Furthermore, it affected teacher attitudes, classroom procedures, instruction, and discipline.

The purpose of Pulliam's (1994) study was to examine the perceptions that computer science educators hold about computer ethics. Of those surveyed, 85% felt that computer ethics was a global problem; yet only 54% reported it was a problem at their institution. A majority of the respondents believed computer ethics should be addressed, and 94% believed that ethical use of computers can be taught. Seventy percent of the respondents indicated that including computer ethics within the curriculum was of extreme importance or great importance. Further findings show that 96% agreed that the subject of copying commercial software should be included in a computer ethics course if one were offered, and 92% agreed that schools should develop and publish a computer ethics policy (Pulliam, 1994).

Leaders within educational institutions are concerned not only with ethical issues in general and how they are affecting student perceptions, but also how this is affecting the learning endeavor itself. Beck and Murphy (1993) report the results of a survey that was administered to 42 university administrators to determine their ethical perceptions. Some respondents made the comment that they had come to believe many problems facing administrators were ethical in nature. Many also expressed the philosophy that educational leadership is an ethical endeavor and that education is a moral enterprise. Leadership requires a vision that draws strength from a basic set of beliefs, and ethical behavior is crucial for success in fulfilling a vision according to those surveyed. The authors conclude by stating that administrators must be equipped to think and act ethically and to develop structures and policies that support consciously chosen, morally sound values and outcomes.

Concerns of educators of the Internet. Educators are particularly concerned with the ethical issues induced by networked computers and Internet access. Over 80% of the nation's colleges and universities are linked to the Internet and are facing problems associated with this technology. College campuses are fast becoming electronic societies (Day & Day, 1996).

The development of computer ethics is in response to a powerful network and Internet environment. This is an environment where people's ideas can be shared or stolen, where intellectual property and software can be used or abused, and where computers can be used to harm or steal, enrich, or improve (Keying In, 1997). The Internet has served to facilitate access to great hosts of information and educational resources; however, it has also served to exacerbate moral and ethical concerns of educators.

While most educational institutions are affected by information technology in some way, more frequent use of computers is associated with higher levels of education attainment (US Department of Education Statistics, 1998). Therefore, colleges and universities provide an ample number of opportunities for unethical behavior.

A few college cases offer a glimpse of the extent of unethical behavior within educational institutions; these illustrate the legitimacy of educators' concerns. The Federal Bureau of Investigation charged a Cornell University student with illegally exchanging child pornography on the Internet. Other campuses complain of sexually explicit images being downloaded onto computers. In one such case, a dean at Camden County College was disciplined for watching X-rated videos on his office computer. In many colleges, access in computer labs to news groups containing explicit images and information is creating problems. At one college, for example, complaints by female students ensued after downloaded information instructing how to torture women had been loaded on computer lab PCs (DeLoughry, 1993). Jones (1998) warns that blocking sexually related Web sites may be necessary to prevent sexual harassment suits for all institutions.

Ethics instruction and education. Information technology is infiltrating educational institutions resulting in benefits as well as problems and potential concerns. Educational leaders are being faced with ethical and moral dilemmas and raising serious questions in these areas. There is a perception that students are receiving inconsistent ethical instruction if they receive any at all. Based upon student ethical perceptions as indicated in the studies analyzed above, educators are apparently justified in their concerns. Meanwhile the Internet is serving to exacerbate the problem.

Kizza (1996) argues that the long-term solution to unethical behavior regarding information technology is education. He theorizes that removing computer crime happens only in a culture that respects privacy and ownership and takes responsibility for the moral decisions it makes. Ethical issues must be communicated; then society must be educated if we are to change unethical behavior.

Rubin (1996) suggests another dimension to the problem, saying, "If we are not competent, there is a greater likelihood that we will engage in unethical actions to obscure our inadequacies" (p. 133). Moreover, he argues there may be attempts to obtain information from unauthorized sources, or to destroy or alter the records of more competent competitors.

According to Peter Tippett, Information Systems professional at Symantec Corporation, the problem is that the majority of technology users are from a generation in which no teachers or guidelines demonstrated accepted codes of behavior (Betts, 1994). DeLoughry (1988) confirms Tippett's conclusion by contending that there is a failure on the part of many colleges and universities to teach their computer science students about the social and ethical responsibilities they will face as professionals. This oversight may be potentially catastrophic. DeLoughry (1988) indicates that the number of computer-related accidents, many caused by not performing responsibly, attests to a deficiency in teaching ethics.

Summers and Markusen (1992) forewarn, "If students and practitioners of a profession are not carefully instructed about ethical issues and concerns relevant to their profession, it is unlikely that they will be guided by them" (p. 92). It is safe to assume that future computing professionals are not the only individuals requiring ethics instruction; all potential users of information technology should receive such guidance.

Responsibility for ethics instruction. It has been argued that education is a critical element necessary to facilitate ethical behavior. The discussion now concentrates upon the responsibility to teach ethics and who should provide such instruction.

A national survey shows that 92% of the population believes children should be taught ethics in public schools. Ninety-four percent of the respondents believe people today are not responsible enough for their actions and feel that the public education system should assist by teaching ethics in classrooms (Franklin-Covey, 1997).

Two surveys were conducted comparing the United States and Canada. Ninety-seven percent of respondents from both surveys strongly agreed that one goal of moral education should be concern and respect for the welfare of others. Both groups felt that moral education should encourage students to think of others, and clearly distinguish moral issues. Both groups also agreed moral education should be handled within the school because home and church alone are not sufficient (Hersh & Pagliuso, 1977).

In a study similar to Hersh and Pagliuso's (1977) analysis, 80% of the respondents agreed that there is a correlation between moral character education and academic achievement. While 84% believed both schools and parents should teach ethics, they also believed that if schools do not incorporate moral development in the curriculum, students may not have the opportunity to develop many necessary traits for successful life. Survey responses also confirmed the community's desire to include moral and character education in public schools (Demmon et al., 1996).

Sadly, many parents are unable to teach ethics for a number of reasons. Some of the reasons include the decline of the family, more mothers in the work force, high divorce rates, and the erosion of the value system of key institutions (Demmon et al., 1996). In other cases, parents may simply be unfamiliar with information technology and the unethical potential that it contains.

Many schools are taking the position that if children are to receive ethical instruction, schools must do the job. In particular, if they do not give proper instruction, students may learn behaviors from their peers or the media or simply act in their own self-interest (Keying In, 1997).

This is not to suggest an either/or educational responsibility or accuse any group of irresponsibility. Character and moral education may be viewed as the primary responsibility of parents; schools can, however, and must amplify the lessons and assume secondary responsibility in ethical education.

Ethics in other disciplines. In light of the conclusion that ethical instruction is a necessary endeavor, another body of literature indicates the potential effectiveness of ethics instruction based upon research conducted in other disciplines.

Walden and Gordon (1988) surveyed mass media law instructors to determine their practices and attitudes about incorporating ethics material into their classes. The respondents overwhelmingly agreed that ethics should be taught in media law courses; however, only 47% of the schools represented required their students to take such courses. Further findings from the survey revealed that 68% of the law instructors devoted less than 10% of their course time to ethics instruction, due to material and time constraints.

Ward, Ward, and Wilson (1996) conducted a study focusing on the effectiveness of ethical instruction with accounting students. They found that ethics instruction had an immediate positive impact on auditing students' perceptions of unethical behavior; indeed, the research also supported the fact that even limited ethics instruction can alter students' perceptions of behavior. The passage of time after instruction appears, however, to be an important element in the students' assessment of behavior and their assessment of how professional accountants would respond. The researchers conclude by proposing that students use the intervening period to internalize the learning experience as well as to increase their level of socialization.

Another study concerning the effectiveness of ethical instruction was aimed at determining the impact of a course in business ethics on the ability of students to identify the presence of ethical issues. The researchers found that a course in business ethics can have a positive effect on student ability to identify the presence of ethical issues and that student sensitivity to ethical issues can be influenced by formal instruction (Murphy & Boatright, 1994).

Cole and Smith (1995) had findings contrary to those of Ward, Ward, and Wilson (1996) and Murphy and Boatright (1994). Student response did not appear to be significantly influenced by whether or not they had taken an ethics course. The researchers believe that a student's ethical values may already be set by the time he or she reaches college. They conclude by suggesting that ethical principles should be included in all courses rather than simply providing an ethics course.

Three hundred ninety-two education professionals were surveyed in the early 1990s. Of those, 53% reported that ethical concepts were taught in a variety of courses. Forty-eight percent of the professionals reported positive effects in attitudes following instruction emphasizing ethical concepts, while only 39% found a similar positive effect on behavior. The researchers conclude by inferring that ethical instruction changes attitude more than behavior (Arnold, 1995).

Teaching of ethics in computer science. It has been asserted that the instruction of information technological ethics is necessary. Sivin and Bialo (1992) affirm, "For technology ethics issues to have an impact on students, they need to be addressed in classrooms and computer labs as part of the instructional process" (p. 16). This instruction should include the respect for privacy, confidentiality, respect for information technology systems as property, respect for intellectual property rights, conflicts between competing rights, and law as it applies to use of information technology.

Kizza (1996) suggests that education should include technology itself as well as ethical considerations. Moreover, security policies should include teaching computer ethics and stressing the professional responsibility to the general public.

In some cases, certification for schools depends upon computer ethics instruction. A study of current business programs in institutions which were members of the American Assembly of Collegiate Schools of Business (AACSB) indicated that 91% had at least one course with a minimum of 10% of the class time dedicated to ethics. In addition, the AACSB has mandated that all schools seeking accreditation expose their students to ethics in undergraduate and MBA programs (Keying In, 1997; Pratt & McLauglin, 1989).

The Computer Science Accrediting Board also requires colleges and universities to be able to document computer ethics and values instruction. As such, computer ethics must be included in the curriculum to receive CSAB accreditation (Pulliam, 1994). An important study was conducted within the computer science field to determine whether computer science educators agreed computer ethics should or could be taught (Pulliam, 1994). Additional topics in the study focused on subject content and methodology. Computer ethics topics included in the study were software piracy, invasion of privacy, inaccurate data, use of computers to commit crime, and viruses. One hundred forty-four full-time faculty, teaching computer science subjects within the researcher's state took part in the survey.

The first research question explored the extent to which faculty believe unethical and inappropriate practices are taking place. Eighty-five percent felt computer ethics is a global problem; however, only 54% considered it a problem at their institution. Of those surveyed, a majority felt that students are more likely to engage in unethical practices than are faculty.

Question number two asked about the perceptions concerning which practices the educators had encountered in the classroom having unethical connotations. Forty-seven percent listed software piracy or the duplicating of copyrighted software as the highest occurrence of unethical behavior. Thirty-eight percent noted situations of plagiarism, copying programs, or copying homework. Hacking and security violations were witnessed by 16%.

The next survey area focused on whether or not educators perceive computer ethics to be an appropriate topic requiring attention in computer science classes; it explored, in addition, which topics should be taught. Ninety-four percent believe that ethical use of computers can be taught. Seventy percent of those surveyed felt that including computer ethics in the curriculum at a college or university level is of extreme importance. Four out of five participants agreed that computer ethics should be taught in a classroom setting and believe that faculty should discuss this topic in other classes as well. The most important topic to be taught, as indicated by 96% of the respondents, is the unacceptable practice of copying commercial software.

The final question investigated the best methodology for teaching computer ethics. The largest group preferred computer ethics as a separate module in a larger course. The second most popular response emphasized the personal example of faculty and staff. The teaching method most favored by 55% of the respondents was class discussion of case studies, although the consensus was in favor of more than one teaching method. A concluding finding showed that 92% of the educators did agree that an institution should develop and publish a computer ethics policy (Pulliam, 1994).

Leventhal, Instone, and Chilson (1992) studied three research questions. They asked first about identifiable patterns of responses to ethical issues among computer scientists. A second question asked does a person's level of technical expertise affect responses to ethical issues? Finally, they inquired how a person's gender affects responses to ethical issues in computer science.

An ethics survey instrument was administered to computer science alumni and current computer science students. The researchers found that doing the right thing becomes more important as students complete their coursework. Subjects with greater levels of technical expertise tended to recognize unethical actions more often as compared to their less-experienced counterparts. Respondents also rated items in the "Right Thing to Do" category the most ethical and items in the "Thievery" category as the least ethical. Finally, the researchers found some differences in responses among men and women. The researchers conclude that based upon the identifiable patterns of responses, apparently computer scientists share a set of attitudes based on specific content, such as government contracts and more general concerns such as thievery (Leventhal et al., 1992).

As preparations for the introduction of ethical components into the curriculum to meet ACM/IEEE curriculum guidelines continued, a survey instrument was administered to all computer science majors at Coastal Carolina University at the beginning of the semester (Sheel & Collins, 1997). The survey results suggested that the university was not doing enough to promote ethical behavior.

After ethical instruction using the textbook Ethics for the Information Age, by Effy Oz (1994), students completed a second survey two years later, in the fall of 1996. The study focused on three questions. What are the current attitudes of students regarding ethical issues? Are there differences in ethical attitudes between students having had a formal ethical component and students who did not? How effective are current strategies that are used to promote ethical behavior?

Surprisingly, the researchers found that a formal ethics component had little impact on students in the computer science program. The researchers conclude that the ethical component is not the problem, but rather the "one shot" approach. The authors agree that ethics needs to be an integral component in all technical courses throughout the students' major courses (Sheel & Collins, 1997).

When ethical concepts concerning computers are initially discussed, many educators erroneously believe that a "one shot" approach may work. They may also believe that rules and regulations encourage ethical behavior. Research indicates that rules alone do not work. Connolly (1995) argues that rules alone will not work because laws and policies are not easily enforceable. Furthermore, careful examination of the ethical dilemmas involving computers suggests that the problems cannot be corrected by a fixed set of rules (Moor, 1985).

Demmon et al. (1996) contend that there are no research findings showing a direct connection between values and behavior. There is an inaccurate assumption, they argue, that teaching moral values will reduce irresponsible behavior. What moral values do provide is guidance for making moral decisions when values conflict. The researchers go on to suggest that youth do not perceive the same social problems as adults and would not likely turn to teachers for advice. Moreover, rules tend to control behavior rather than shape character. They conclude, students should be taught not just to obey rules, but rather how to make sound ethical decisions.

Ethics instruction. To enable students to make wise ethical decisions, it is necessary to make them active participants instead of passive observers in the making of moral choices (Obrien, 1989). Ethical instruction appears to be the most effective means of facilitating prosocial conduct since one goal frequently proposed for courses in ethics is that of changing student behavior. Consequently, the content of ethics courses should not be about what is right or wrong but how to recognize when there is a problem (Keying In, 1997). Callahan and Bok (1979) insist that there is no point in teaching ethics unless it guarantees improvement in student conduct.

The goal of changing behavior as the most effective means by which students increase ethical conduct is one that has been studied by several researchers. Miller and Coady (1984) believe that individuals move through their work ethic stages of development much like the moral development stages presented by Kohlberg and Piaget.

Bickel, Larrondo-Petrie, and Bush (1992) developed an instrument called Ethical Dilemmas in Computing Test (EDICT) to determine a subject's stage of moral development through analysis of responses to computer-related scenarios involving ethical decisions. The researchers were interested in developing effective methodologies for teaching computer ethics by studying behavior.

The three areas of concentration were computer ethics, philosophical ethics, and moral development. The researchers used Kohlberg's six stages of moral development. These include: Level 1: Preconventional moral reasoning, Stage 1: Obedience and punishment orientation, Stage 2: Naively egotistic orientation; Level II: Conventional moral reasoning, Stage 3: Good boy/girl orientation, Stage 4: Social system and legal authority orientation; and Level III: Post-conventional moral reasoning, Stage 5: Contractual legalistic orientation, and Stage 6: Universal ethical principle orientation.

The researchers found that class discussions either changed people's perception of the proper course of action or made them sensitive to factors not previously considered. Seventy-eight percent of the subjects changed their minds on at least one answer, indicating that being presented with other viewpoints can persuade people to change their minds.

A second finding points to a relationship between moral judgement and conduct. This finding is consistent with what Kohlberg and Kandee (1981) discovered, that individuals who use a higher stage of reasoning become more predictably prosocial in their behavior. Bickel et al. (1992) conclude by recommending that any computer ethics course concerned with enhancing prosocial behavior should monitor the reasoning of participants. This requires developing classroom techniques to move students to higher levels of moral reasoning.

Petrick (1992) examined Kohlberg's model of individual moral development comparing it with a model of organizational moral development. The study showed that justice and individual rights are moral ideals requiring a balance because they are often in tension. Balanced judgment among competing interests shapes organizational character; this, in turn, determines the rightness or wrongness of behavior.

The Petrick (1992) study confirmed the researcher's hypothesis that specific structure policies and procedures need to be implemented in order to institutionalize ethics. Additional findings include confirmations of the fact that large organizations are more likely to institutionalize ethics policies and programs than smaller ones, and that those systems that have institutionalized a full range of ethics-related programs are most likely to achieve a higher level of organizational moral development. The researcher also found, consistent with prior studies, that one-shot ethics training programs focusing exclusively on "regulatory compliance do not provide employees with the tools to identify, clarify, analyze, and resolve ethics issues" (p. 334).

While many researchers found that behavior is significantly improved following instruction, others did not reach that conclusion. Arlow and Ulrich (1983) indicated in their work that, while exposure seems to sensitize students to issues of business ethics, this increased awareness diminishes over time once the exposure has been removed. Awareness about ethical problems is a positive attainment concludes Baumhart (1968); however, there is no evidence found in his study, that decision-making is more ethical as a result of a college ethics course.

Undergraduate and graduate business students at Iona College were surveyed in the early 1980s. The results of that study showed, while students studied the belief systems underlying their ethical behavior, they were not influenced in a statistically significant way by ethics courses. This raises a question of whether there is a diminishing marginal utility based upon resistance to previously acquired attitudes concerning change or whether additional courses simply reinforce beliefs that have been previously compounded by repetition (Baron, et al., 1984).

Impact of a policy. As discussed thus far, ethical instruction within education is critical to the moral success of future societal members. Although ethical concepts are taught in many courses, there is a perceived need for something more. It is a necessary and responsible act on the part of a college to protect students, employees, and others from the negative aspects of an increasingly powerful information technology (Kallman, 1992).

Johnson (1991) stresses the importance of working out ethical issues surrounding computers. There must be an understanding of the nature of human relationships, an understanding of institutional purposes involved, and an understanding of the norms of behavior that have been operative (Johnson, 1991).

R. B. Quinn, legal director of the First Amendment Center at Vanderbilt University in Nashville, states that there is little the government can do concerning unethical behavior with computers. The common theme is to have a policy that causes those who abuse the system to lose their access. The researcher recommends that the highest priority is to establish acceptable policies concerning computer use and access to objectionable materials on the Internet (Gregory, 1994).

Hunt and Paplewis (1989) also argue that educators have a responsibility to establish policies for ethical use of computers. They conducted a study of four school districts and 10 site administrators and found that most of the school districts did not have board polices or regulations governing the use and copying of software. In those districts that did have policies, administrators often were unaware of their existence, or they were often not followed at the site or classroom level. The researchers conclude that most school administrators are lacking in their working knowledge of ethical computer use.

Moor (1985) believes that computers have enabled us to make new choices; however, there is a "vacuum" or absence of policies, which provide guidance about how to make these choices. Further compounding the issue, the invisible nature of computer technology also tends to generate policy vacuums.

Johnson (1994) asks whether the vacuum in policies should be filled with laws or something else. She believes that moral ideas often contribute toward and shape the character of our laws, and suggests that ethical issues surrounding computers are a "new species of old moral issues" (p. 10). Her conclusion, then, is that rules, policies, attitudes, and conventions will make all the difference whether the computer's potential is exploited for good or evil.

Society and organizations must depend upon the personal integrity of individuals, which creates a need for education, resources, and examples. "Education is needed for students, faculty and staff, not only about the importance of intellectual honesty, but also on the laws, rules, procedures and expectations of society and the institution regarding intellectual property" (Connolly, 1995, p. 87). Facilities containing adequate resources are also needed; these would eliminate the need for pirating. There is also a need for faculty members to demonstrate ethical computing habits, insists Connolly (1995).

Connolly (1995) further poses a question and provides an answer, "Why would a college or university bother to spend the time and energy to promulgate such a policy? Two reasons come to mind—liability and environment" (p. 87). A computer policy is a basis for mitigating liability if an employee or a student is found acting counter to the established guidelines and regulations.

Computer use has developed so rapidly that it becomes difficult but important for institutions to take proactive steps rather than respond reactively. Budden (1984) found in an early study that nearly 90% of responding colleges were highly concerned about developing policies and guidelines for introduction and use of computers in the classroom. He also found that respondents indicated education and training in the ethical dimensions of computer use was critically important and supported strongly by management.

It has been recommended by researchers that educators must consider how education might be affected by information technology and how ethical issues relate. Other researchers have also supported a proactive response. If critical, technical, and policy issues related to security are not prepared for in advance, then effective security will be missing; this will result in reduced integrity and credibility of information networks (Hoffman & Clark, 1991).

Johnson, writing in 1991, noted a lack of policy concerning access to data, ownership of software, and privacy of electronic mail. She recommended board-adopted policies that would cover computer and on-line resources much the same as policy provisions for any other educational resources. It may be worth noting at this point that in spite of earlier studies determining a need for policies, many educational institutions still have not developed these guidelines.

The Internet, in the last few years, has greatly increased the need for computer ethics policies. Johnson in a perceptive 1994 article suggests that the Internet or "cyberspace" has existed for some time in telephone lines, which are privately owned. The problem arises because this medium has been extended to computers, and we have never had a public discussion about how cyberspace might be set up. Should it be public or private? Should it be one or many systems? Finally, should cyberspace be a commercial, educational, personal, or governmental responsibility?

Connolly (1995) sees cyberspace as the "ultimate in freedom and rugged individualism . . . no police, few laws, great flexibility and power, and unlimited freedom" (p. 86). Johnson (1994) recommends that, while there is a technological versus human approach to handling ethical problems, the emphasis should be on the human approach. This would include better legislation, attitudes, conventions, and encouragement to organizations to become more responsible for computer technology and education (Johnson, 1994).

One of the major motivational factors for many organizations to develop computer ethics policies is to protect a company from legal litigation. This may be achieved by drafting a policy for acceptable Internet behavior. An employee comment made offhandedly and accidentally can make a company liable. Thus, a computer ethics policy is the best way of preventing harassment suits, libel issues, and other legal problems (Weston, 1996).

Saunders (1994) suggests that virtual communities, which exist through the Internet, require rules of conduct just as any other society. He believes that organizations need to be proactive in identifying and discussing ethical ramifications of Internet access. The best method of addressing many of the ethical issues raised is through the use of an acceptable use policy as a means of clarification. Marker (1996) also confirms that, increasingly, schools are electing to develop and enforce acceptable use policies.

Day and Day (1996) reveal the current situation in many colleges and universities. If a student downloads certain material, for example, the professor may call it pornography while the student insists it is literature. Without a computer ethics policy to deal with issues such as this, the hands of educators are tied.

Among the students who Day and Day (1996) surveyed, a majority favored a computer use policy to regulate and outline ethical behavior. It becomes an educational dilemma because while these particular university students appeared in favor of some type of censorship, the broader population does not (Day & Day, 1996).

The National Education Association (NEA) has focused extensively on development of acceptable use policy templates for educators and students. The group feels that filtering or blocking software has been ineffective and difficult to govern. It is their belief that students must have access to the Internet and its valuable resources. Students should also be allowed freethinking in an atmosphere of free inquiry, unencumbered learning and spirited exchange of ideas.

The NEA confirms that there is a lack of statistics or research showing the extent of student exposure to indecent material on the Internet. When occurrences happen, educators tend to seek community input in devising Internet use policies. "Various studies have shown that blocking software and filtering software have serious technical limitations and provide a false sense of security." The NEA suggests that the only reasonable answer is the implementation of acceptable use policies (Congressional Testimony, 2-10-1998).

Because of the dramatic increase in computer use, institutions of higher education are responding to the concern of educators who are attempting to remedy the problems stemming from information technology. A survey was conducted in June of 1996 in 660 two- and four-year colleges and universities across the country. The study showed that 67% of all undergraduates have access to the Internet, up from 6% in 1995. Seventy-nine percent of the campuses surveyed have an institutional presence on the Internet, up from

55% in 1995. Community colleges were found to make a far larger proportion of the institutionally owned computers available for student use than research institutions.

Further findings from the study revealed that a growing number of colleges are turning to user fees as one way to manage continuing costs. In addition, a growing number of institutions have formal policies for students, faculty, and staff regarding unauthorized duplication of computer software. Finally, 69% of the responding colleges and universities have formal policies compared to 30% in 1990 and 57.7% in 1993 (Green, 1996).

In 1997, the University of California at Berkeley began a class entitled "Ethics, Access and Equity in Technology" as a means of enabling and equipping educational administrators with computer ethic guidelines. The topics studied included fair use policies, copyright law, intellectual property, profanity, pornography, and on-line etiquette. All those attending developed a fair use policy to take back to their schools.

The State of California Department of Education has also approached this issue by mandating that all schools have a computer use policy. The policy is considered a computer contract made between the student and the school. The student agrees to act within certain parameters of behavior while using the Internet and computer applications, and the document is signed by both student and parent (Business Wire, 1997).

Acceptable use polices do work quite well. In one particular case, a Northeastern University student placed sexually explicit material on his home page. The university's administrative personnel were able to force the student to remove it only because the university acceptable use policy prohibits transmitting or making accessible offensive material (Cobb, 1996).

In other cases, when universities have attempted to remove information, students claim censorship while administrators insist it is editorial policy (Winn, 1996). The Electronic Frontier Foundations alludes to the fact that universities would have a battle to challenge the constitutional right of free speech if they started to censor. Notre Dame, as have several institutions, has started using disclaimers that they do not take responsibility for content. This works particularly well in situations that exist in the gray areas surrounding a computer ethics policy (DeLoughry, 1995).

Educators have good reason to be cautious; the government, however, does provide some measure of protection. A university would be responsible for defamation by students only if the university had knowledge of the statements and failed to take appropriate action. Pavela (1996) concludes an article advocating proactive action by stating that we must do a better job of educating system users about their copyright responsibilities. If we fail to do this, it will not be long before we see significant changes in copyright law including potential new liabilities for system operators and restrictions on the scope of fair use. Several such bills have already been introduced in Congress.

It becomes apparent that educating computer users concerning how to make the best ethical decisions is both necessary and beneficial to society. The research reviewed indicates that personal computer ethics policies and instruction may very well be the only viable solution given the political and legal battles that occur due to the legislative attempts and conflicting views of various interested groups.

To facilitate ethical instruction, a computer ethics policy is viewed as a guiding framework that provides a foundation for ethical precepts to be communicated to users and also serves as a starting point for organizational leaders. A computer ethics policy provides guidelines, sets rules of ethical conduct, and facilitates prosocial behavior. Thus a computer ethics policy can provide a guiding framework for organizational leaders who may use a policy as a crucial component for educational instruction.

Behavioral Models

The body of research and empirical studies concerning behavioral theories may assist educational leaders in their efforts to develop computer ethics policies and ethical instruction. These theories provide insight into the underlying factors that elicit certain behavioral manifestations by computer users. As a result, components of computer ethics policies may be written specifically to address the underlying factors revealed by such studies. Three particular theories have been identified through a review of literature as particularly useful in the analysis of human behavior and computer use.

Fishbein Behavioral Intention Model. Fishbein's Behavioral Intention Model is based on Dulany's (1961, 1964) theory of Propositional Control (see Appendix A). That theory states that a person's intention to perform is based on attitude toward performing the behavior in a given situation, norms governing that behavior, and motivation to comply with those norms. Fishbein's model expands to include behavioral intention, situational specificity, and normative beliefs.

The primary assumption of the model is that behavioral intention is an immediate antecedent of overt behavior. An individual's intention to perform a given action in a particular situation is highly specific, and execution of behavior must be entirely under the subject's volitional control.

Fishbein's (1963) model is composed of the following concepts: a) individuals hold certain beliefs about any given object, b) associated with each object is a mediating evaluative response or attitude, c) these evaluative responses summate through the mediation process, and d) are associated with an attitude about the object. Thus, on future occasions the object will elicit this summated evaluative response or attitude.

Fishbein joined with Ajzen (1972) in a study to determine if one of the factors influencing a person's beliefs about what others expect him to do is his perception of the other's attitude toward the act. They found evidence supporting this hypothesis. They also found that a person's behavioral intentions in the hypothetical situations were related to attitudes toward the behaviors and normative beliefs.

Further support for the Behavioral Intention Model was provided through a study by Wilson, Mathews, and Harvey (1975). Findings in the study indicated that normative beliefs are more important than attitudes in predicting intentions. They reported a strong association between behavior and behavioral intention, thus suggesting that the BI Model indirectly predicts behavior, as anticipated. Based upon the Behavioral Intention Model the Theory of Reasoned Action was developed.

Theory of Reasoned Action. Fishbein and Ajzen's (1975) Theory of Reasoned Action posits that the critical key to predicting behavior lies with intentions, which are shaped by attitudes toward the behavior. Social norms and beliefs are ultimate sources of attitudes and norms. The attitude is focused on the act itself rather than on the target of the act.

The theory is based on the assumption that human beings are usually quite rational and make systematic use of information available to them. Behavior follows logically and systematically from whatever information that happens to be available.

Behavioral intention is a function of two basic determinants: attitude toward performing the behavior and a subjective norm regarding the behavior. Attitude toward performing a given behavior is a function of two components: the belief that performing the behavior will lead to certain consequences and the person's evaluation of those consequences. Attitude is generated toward performing the action rather than toward an object, person, or situation.

The second determinant of attitude is the social component. The subjective norm is an individual's perception of whether most people who are important to the individual think that he or she should perform the behavior in question. All other sources of influence on behavior are mediated by the two predictor variables of attitude toward the behavior and subjective norm.

Theory of Planned Behavior. The Theory of Reasoned Action was expanded to become the Theory of Planned Behavior (see Appendix B). The central factor of this theory is the individual's intention to perform a given behavior. Intentions are assumed to capture motivational factors that influence behavior. These are indications of how hard people are willing to try and how much effort is exerted in order to perform the behavior (Ajzen, 1985, 1988).

This theory postulates three determinants of intention: a) the attitude toward behavior and the degree to which a person has favorable or unfavorable evaluation of behavior; b) the social factor, or subjective norm, is the perceived social pressure to perform or not to perform the behavior; and c) the last determinant is the perceived ease or difficulty of performing the behavior based upon prior experience and anticipated obstacles.

The original derivation of the Theory of Planned Behavior (Ajzen, 1985) differed in two major respects from the present model (Beck & Ajzen, 1991). It defined attitude, subjective norm, perception of control and intention in terms of trying to perform a given behavior rather than in relation to actual performance. Second, the original formulation of the theory postulated interactions between perceived behavioral control and intention and between perceived behavioral control and attitude.

The later study indicated that the Theory of Planned Behavior was clearly superior to the Theory of Reasoned Action, indicating that intention to perform dishonest behaviors are strongly affected by beliefs about potential obstacles and opportunities (Beck & Ajzen, 1991).

Theory of Deindividuation. Departing from the theories of Reasoned Action and Planned Behavior, a final theory is discussed. The Theory of Deindividuation (see Appendix C) appears to be most appropriate for the study of computer user behavior and ethics. Unlike the other two theories, the Theory of Deindividuation identifies the presence of two subsystems, and takes into consideration the tension that exists between personal identity and social identity of an individual.

The review of literature indicates that the primary motivational factor involved with occurrences of deindividuated behavior, is the individual's desire to engage in antisocial conduct not normally permitted. Although individuals can use their individual beliefs, standards, and experiences to guide their behavior, they often monitor and define their behavior based upon comparisons with other members of society.

As individuals seek to compare their behavior with others and maintain social identity, they may seek out other groups with which to identify. The computer enhances networking with others through e-mail and encourages interactions through bulletin boards, list serves, chat rooms, and other Internet features. This makes this process much easier by assisting in the ease of identification and connection to other groups. As individuals immerse themselves in the computer world and identify with particular groups, the internal responsibility to establish a sense of rationality of individual behavior becomes less significant or is ignored altogether. Thus, the individual becomes deindividuated.

By the same token, the computer may provide assistance to individuals wishing to minimize their social identity in favor of personal identity. By immersing oneself within the computer, absences of others that may evaluate, criticize, or punish may be experienced. The individual may be influenced by the anonymity that computer users can often experience through the use of personas, lurking, and other common behaviors that have been studied by computer science, communication, and other scholars. Computer use also can encourage perceptions of freedom from the individual and group influences of others that normally exist in the world apart from the computer. As a result, the individual can become a deindividuated individual.

The study of deindividuation first began with the work of LeBon (1895) who investigated crowd behavior. He saw how individuals were able to "submerge" themselves in a group, thus becoming anonymous and losing their conscious personality. This feeling of being unseen and not personally identifiable enabled the individual to express primitive feelings and impulses.

This work was continued by Festinger, Pepitone, and Newcomb (1952), who first coined the term "deindividuation," describing the situation in which individuals are not seen or paid attention to as individuals. They concluded, "Anyone who observes persons in groups and the same persons individually is forced to conclude that they often behave differently in these two general kinds of situations" (p. 382).

The primary motivational factor leading to deindividuation is for release of behavior usually not permitted. In some cases, behaviors that individuals desire to perform but are unable to do because of internal restraints become possible under deindividuation. This in turn leads to a greater attraction to and satisfaction with the group.

The study by Festinger et al. (1952) was conducted to determine the relationship between frequency of negative attitudes toward others, the ability to identify who said what negative remarks, and the relationship between frequency of negative attitudes and attractiveness of the group. The study showed that deindividuation does tend to result in a reduction of inner restraints resulting in indulgence of behavior usually restrained from, and contributes to an increase in attractiveness of the group.

Continuing the study of deindividuation, Ziller (1964) found that the phenomenon occurs more as an internal psychological phenomenon when persons become subjectively undifferentiated from those around them. The next researchers to examine deindividuation were Singer, Brush, and Lublin (1965) who suggested that the factor of "lost self-consciousness" and reduction in feelings of distinctiveness were essential to deindividuation (p. 356). A usually undesirable act could be engaged in with a greater attraction to the group allowing such behavior.

The researchers allude to the fact that, based upon the status of a hypothetical construct, deindividuation may be inferred only if two consequences have occurred: the person has engaged in a usually undesirable act, and his or her attraction to the group has increased. While these two factors do not always cause deindividuation, the emergence of these behaviors provides a sounder basis for the inference of deindividuation (Singer et al., 1965).

Singer et al. (1965) conducted an experiment with the following hypotheses. The first states that groups in settings with cues to identifiability will have a higher proportion of conformers than groups whose settings provide fewer cues to identifiability. The second hypothesis, is when two people who have feelings of a lack of identification (deindividuation) and do not conform are compared with nonconformers who feel identifiable, then the former should show a greater attraction for their group, more interest in proceedings, greater personal satisfaction, and less anxiety.

The manipulation of identification was constructed through attire. The high-identification group wore name tags and proper dress clothes, while the low-identification group had old clothes, large lab coats, and no name tags. The results showed that the decreased conformity in social norms, increased conformity to group norms, and increased attraction to group in the low-identification group were indeed manifestations of deindividuation. However, the researchers discovered the possibility of some extraneous confounding variables as possible limitations to the study (Singer et al., 1965).

The presence of confounding variables led to the second study in an attempt to uncover the true manifestation of deindividuation. The subjects in nine groups were given the task of discussing a taboo topic, while four other groups discussed a non-taboo topic. The experimenter presented a definition of pornographic literature as established by the US Supreme Court. The task was to inspect examples of literature and decide whether it fits into the rule. The non-taboo group read and discussed a definition of liberal education.

The main measure was a tally of the number of statements in which obscene language was used; obscenity was defined as the use of certain words. This ended with a group-feeling questionnaire. The results of the study showed significant differences with the low identification group using obscene words more frequently than the high identification group. It was also revealed that the people who found the group most attractive were in the group conditioned to produce the most deindividuation.

The researchers conclude by suggesting that deindividuation is a group phenomenon only when or to the extent to which the group provides an appropriate environment and models for behavioral imitation and contagion. Singer et al. (1965) further propose that "individuation" be viewed as a subjective differentiation of self from other social objects in the field. As such, individuation is desirable within a supportive social environment, but deindividuation is sought as defense against a threatening environment.

Zimbardo (1970) was the next researcher to test the Theory of Deindividuation. His studies emerged from the dissonance theory with consistency, commitment, and responsibility as the dynamics involved. Individuals strive for consistency because this is viewed as the norm within our society. If one's behavior is not comparable to others around for reference, then the individual must establish the rationality of his or her behavioral commitment.

> Thus, consistency becomes a self-imposed principle in order for the individual to maintain a conception of himself as a normal member of society who, in behaving as others expect him to, gains their social recognition (the most potent of all reinforcers) as a rational decision-maker, whose decisions help him to control his

environment. (Zimbardo, 1969, p. 280)

Freely making a commitment for which an individual assumes responsibility individuates the decision-maker. With readiness to enter into a contractual agreement with consequences for which one must be liable, an individual sets himself in opposition to all who refuse to act individually and thus separates himself from tribal ties to undifferentiated (safer) group action (Zimbardo, 1969).

Zimbardo (1969) asserts that we should examine the following:

> Start by assuming that life represents the conversion of matter into energy; that initially this energy is undifferentiated and uncontrolled in its onset, direction, intensity, and terminal properties. Such a force is dangerous to the individual organism because it could be turned in on itself and become self-consuming and destructive. Likewise, it is dangerous for society because it makes every member potentially subject to the transient (demonic) impulses of all others. To contain this energy from destroying the substance which creates it or the environment which nourishes it, forms, structures, and institutionalized systems of control have evolved. (pp. 253-254)

The mechanisms used to control behavior are ego identity, social and physical reality, temporal ordering of experienced events and time, history and logic, legal systems, and religion. These "cognitive" systems guarantee the existence of self and society by encouraging individuation (Zimbardo, 1969).

Output behaviors described thus far are more likely as an individual feels more anonymous. If others can not identify the person, they may not evaluate, criticize, judge, or punish. Moreover, the loss of identifiability can be conferred by being "submerged in a crowd, disguised, masked, dressed in a uniform like everyone else, or by darkness" (Zimbardo, 1969, p. 255).

The responsibility factor one feels for having engaged in antisocial behavior may be insignificant in situations in which the behavior is shared by others or by conditions that obscure the relationship between action and effect. The responsibility factor may also be decreased when a leader is willing to assume all accountability for the antisocial behavior.

Zimbardo (1969) found that the presence and size of a group aids member anonymity and shared responsibility. This can also serve additional functions by providing models for action, generating physical activity, or triggering behavior in a given direction. The state of arousal additionally increases the likelihood that aggressive behavior will be released and, in the situation cues normally causing inhibition may go unnoticed.

Deindividuated behavior must have the property of being a high-intensity manifestation of behavior, one which observers would agree is "emotional, impulsive, irrational, regressive, or atypical" for the participant in the given situation. The behavior must also be unresponsive to the situation, target, victim, or states of self that normally evoke a given response. Under individuating circumstances, the person is normally responsive to many sources of feedback. With deindividuating ones, there is a screening effect in which the only source of feedback allowed into the system is self-reinforcing.

The behavior will be difficult to terminate due to the self-reinforcing aspect and lack of consideration of external stimuli. At some point of intensity, termination will be intolerable; those attempting to terminate may be attacked and destroyed by the deindividuated mass. The behavior may be terminated at some point by any one of the following: a change in the state of an individual (fatigue), a change in target object or victim, or a change in the state of an instrument of action or environment.

Certain behavioral input variables are relevant only when a group is present. The presence of others stimulates contagious behavior caused by sensory awareness of others rather than cognitive pressures toward group conformity. There is a total loss of conformity to relevant norms of any reference groups not physically present—this is the antisocial feature. Attraction to the group and group interaction break down during the highest level because each member responds autistically only to himself (Zimbardo, 1969).

To test his assumptions, Zimbardo (1969) administered an experiment. Anonymity was induced in half the subjects by making them unidentifiable, by never using their names, and by having the experimental task done in the dark. For subjects in the control group, individuality and identifiability were emphasized. The hypotheses were that conditions of deindividuation should lead to greater levels of aggression (shock duration) than the conditions of identifiability and that this aggression should increase over trials for only the deindividuated group.

The outcome of the study provided evidence to support the hypotheses. Deindividuation had a significant effect on aggressive behavior. The total duration of the shocking was twice as much for the deindividuation group as for the individuation group, and there was an increase of aggression over repeated trials.

> Deindividuated behaviors are more likely to be released when loss of personal identity occurs in a group setting than when the individual has no group support and is made to feel self-conscious by obvious cues of difference from those observing him. Furthermore, where anonymity operations conceal the identity of the members of a natural group from each other, the individual feels isolated from his friends and cut off from this source of social support. (Zimbardo, 1969, p. 279)

Diener (1979, 1980) contributed to the theory by adding that when one's attention is drawn outward toward the group, one will rely less on internal standards and more on external cues. Since deindividuated persons are less likely to self-regulate their behavior with long-term norms, they are more likely to perform disinhibited behaviors. A marginal effect occurs; as more people are added, each additional individual will have less impact than the ones added earlier.

The primary components of deindividuation compiled thus far from the researchers include the group variable, anonymity, arousal, altered responsibility, altered self-awareness, and cognitive set. The group variable implies that it is an important part of deindividuation. Large groups are perceived by both actor and onlooker as a product of a whole collective rather than as individual persons. Thus, deindividuation is a cause, not a result, of unrestrained behavior in groups.

The second factor, the size of a crowd and feelings of anonymity, significantly correlate even without masking identity. This shows that mere immersion within a large group makes one feel less identifiable (Diener et al., 1974a). Anonymity does not automatically cause antisocial behavior but liberates normally inhibited behavior. Behavioral effects of anonymity depend upon the participant's perception of the possibility for reward or punishment.

Arousal tends to express itself through aggression and an increased attraction for the group (Festinger et al., 1952). A lack of responsibility releases uninhibited behavior; external manipulations may not influence a person's feelings about one's behavior but may help release him or her from perceived external restraints. This contributes to a reduction in self-awareness, and individuals may justify some behavior at the onset, causing them to cease monitoring their actions (Diener, 1977).

Further evidence indicates that the less one knows about a person, the more likely one will behave unethically toward that person. The more distant or anonymous a victim is, the more readily subjects harm that victim (Milgram, 1965). Individuals are also more likely to help others when they know something about them or when others are individuated (Emswiller, Deaux, Willits, 1971).

Worchel and Andreoli (1978) reported evidence that when individuals are anticipating aggressive interaction, the subjects tend to deindividuate the target by recalling less unique information about him or her than when they are anticipating a friendlier encounter. The more deindividuated persons are, the more likely others will behave negatively toward them, and they will more likely become the targets of socially inappropriate behavior. These studies also support the hypothesis that intergroup discrimination decreases when the out-group is individuated (Wilder, 1978).

More recent studies testing the Theory of Deindividuation provide even stronger support. Dodd (1985) did an experiment with college students to demonstrate the concept of deindividuation. Three classes were composed of students from a maximum-security prison, and the remaining participants were traditional college students. The deindividuation variable was operationalized through a stimulus question and measured through the subjects' response. The stimulus question in the study asked, "If you could be totally invisible for 24 hours and were completely assured that you would not be detected, what would you do?" (p. 90).

The results from the study showed that 36% of responses were antisocial. For research purposes, antisocial behavior was defined as injuring others or depriving them of their rights. Nineteen percent of the responses were non-normative, which was defined as behavior violating social norms and practices without specifically helping or hurting others. Thirty-six percent were neutral and only 9% prosocial, demonstrating behavior intending to benefit others. The response content showed that the most frequent responses were criminal acts (26%), sexual acts (11%), and spying behaviors (11%).

Interestingly, no significant differences were found between the prison students and the campus students regarding either kinds of responses or extent of their antisocial content. The researcher concluded that even average, well-adjusted students are capable of antisocial behavior. This led to the further conclusion that deindividuation occurs more frequently based upon the important role of situational conditions, such as perceived anonymity, rather than personal traits or characteristics.

Several studies have taken into account deindividuation and group composition and dynamics. In one such study, the emergence of "group mind" was found to cause different individuals who comprise the collective to lose their distinct personalities, becoming a homogeneous, highly emotional mass. Moreover, group mind leads to primitivation or regression, which spreads throughout the group. When deindividuation occurs, it leads to an expression of normally inhibited behavior. People also tend to be attracted to the group, thus enabling them to overcome social restraints.

Findings from this study proved that abundant aggressive content makes people pay close attention to the content. They remember the material better, while remembering less who said what. To resolve conflict over the expression of hostile feelings, subjects ceased paying attention to each other. Thus, when they achieve a critical level of "submergence" in the group, they are able to "break" the conflict (Cannavale, Scarr, & Pepitone, 1970).

Large heterogeneous groups also contribute to deindividuation through anonymity. Fisher (1975) found that crime rises in correlation to group size. Individuals engaging in antisocial behavior within a small town are unlikely to meet others with similar inclinations. In contrast, large cities allow the increased probability of interaction between individuals with deviant patterns. This allows for the "formation of large deviant groups or subcultures which may then disseminate information, attract newcomers, and compete for political power" (Sadalla, 1978, p. 282).

There has also been exploration of the concept of group salience and the potential positive consequences of deindividuation. Turner (1982) believes that self-concept may be divided into two subsystems—personal identity and social identity. The two are independent of each other, and one may operate to the exclusion of the other. As such, the decreasing of personal identifiability does not destroy identity but increases the salience of social identity. Deindividuation produces effects by altering the relative salience of personal and social identity and by manipulating adherence to personal standards or social norms. Turner (1982) concludes, deindividuation is not always antisocial, but depends on group norms and context.

The concept of social identity involves the distinction between deindividuation as immersion and deindividuation as anonymity. Deindividuation as immersion in a group increases the salience of social identity. Attention switches from the individual to the group, and adherence to group norms increases. In contrast, the result of deindividuation as visual anonymity depends on the context in which it occurs and the operating group norms.

Deindividuation of individuals in isolation decreases the salience of social identity and, consequently, decreases adherence to group norms. When deindividuation is used in the original sense to denote submergence, evidence shows it produces its effects by increasing the salience of social as opposed to personal identity and not just through destruction of personal identity.

To test this hypothesis, Reicher (1984) organized an experiment. Findings indicate no evidence to suggest that immersion within a group or visual anonymity lead to increases in antisocial activity or decreases in prosocial activity. Therefore, the results support the hypothesis that deindividuation acts by manipulating the salience of social identity. Crowd behavior is determined by the nature of in-group norms, and the supposed state of anonymity, far from occurring in crowd conditions, occurs only when an individual is separate from the crowd. Deindividuation or anonymity associated with immersion in a group does not weaken social norms, but can act to enhance the salience of the group and the relevant norms.

The behavioral theories discussed thus far may assist educational leaders in their efforts to develop computer policies and ethical instruction. These theories provide insight into the underlying factors involved with computer user behavior. Particularly well-suited for the study of computer ethics is the Theory of Deindividuation.

Deindividuation and computers. Some have noted that the computer is often considered one of the most socially distancing and impersonal modes of communication and that computer-mediated communication represents only one step above no communication (Matheson & Zanna, 1988).

Kiesler (1986) states, "Because computers break down hierarchies and cut across norms and organization boundaries, people behave differently when using them" (p. 46). New technology tends to have an unintended social effect because it permanently changes the way social and work activities are organized.

The computer has become a communication tool, and is referred to by some individuals as a social activity. In computer-mediated communication, there is limited information concerning the social context. Without nonverbal tools, it becomes difficult for communicators to alter the mood of a message. Thus, individuals tend to focus more attention on the message itself rather than on the individual communicating the message.

Participants who communicate by computer also feel a greater sense of anonymity and detect less individuality in others than they do when conversing by phone or face-to-face in many cases. They may express less empathy, less guilt, or less concern over how they compare to others and experience less influence by social norms. Moreover, when social definitions are weak or nonexistent, communication may become unregulated, more extreme, impulsive, and self-centered (Kiesler, 1986).

Information technology also has the ability to break down hierarchical and departmental barriers, standard operating procedures, and organizational norms (Kiesler, 1986). Once people have electronic access, there is a tendency for their status, power, and prestige to be communicated neither contextually nor dynamically. As a result, charismatic and high status individuals may have less influence, and group members may participate more equally in computer communication.

Electronic communication tends to seem impersonal due to a lack of contextual cues. Computers also tend to encourage individuals to be self-absorbing and to give quick responses. This reduction in self-awareness gives an increased feeling of being submerged in the machine and is very much the same as when people are submerged in a group or deindividuated (Kiesler, Siegel, & McGuire, 1984).

Kiesler (1986) found that group participants in a study spoke more uninhibitedly, engaging in name-calling or making personal remarks to others more often when using the computer than when in face-to-face communication. A positive outcome, however, was the finding that computer-mediated groups were more efficient because participants told others what they preferred in fewer words.

In a similar study by Sproull and Kiesler (1986), uninhibited behavior was reported as increasing while e-mail messages were exchanged. The occurrence of "flaming" or negative remarks was recorded a mean of 33 times as opposed to 4 times a month for face-to-face messages. The second kind of uninhibited behavior noted was the increased willingness of individuals to communicate bad news or negative information.

The third discovery was the "flouting" of social conventions or blurring of distinctions between work and play. E-mail also reduced the social context cues and provided information that was relatively self-absorbed. In addition, participants were undifferentiated by status, were more uninhibited, and behaved more irresponsibly more often on e-mail than face-to-face conversations. As was discovered previously, a positive effect could be found; uninhibited behavior led to an increase in new ideas, similar to brainstorming, as a result of released inhibitions (Sproull & Kiesler, 1986).

In an earlier study, groups of individuals were asked to reach consensus on a choice-dilemma problem. The researchers used three different communication contexts: face to face, anonymous computer use, and nonanonymous computer use. The results showed that in all three experiments computer-mediated communication had significant effects on communication efficiency, participation, interpersonal behavior, and decision-making. The computer-mediated groups took longer to reach consensus than face-to-face groups due to the additional time needed to key messages using the keyboard.

Individuals in the computer-mediated groups were more uninhibited than participants in the face-to-face groups, as measured by verbal behavior. Verbal behavior was defined in terms of the frequency of remarks containing swearing, insults, name-calling, and hostile comments. The researchers concluded that the frustration from discussing problems inefficiently could have caused participants to become angry and thus more extreme in their decision-making and more uninhibited (Kiesler, Siegel & McGuire, 1984).

Researchers in another study sought to determine if computer-mediated communication changes group decision-making (Siegel, Dubrovsky, Kiesler, McGuire, 1986). It was hypothesized that the absence of social context information and social feedback leads to uninhibited behavior. This results from the technical and social characteristics of computer-mediated communication that hinders communication of social context information. A depersonalization of the situation and behavior occurs, thereby, causing submergence in the technology rather than submergence in the group.

These researchers believe that computer-mediated communication includes some of the conditions important for deindividuation. They predict that computer-mediated, as compared to face-to-face, communication will reduce feelings of embarrassment, guilt, and empathy for others. They further believe that there will be less social comparison with others and a reduction in fear of retribution or rejection. Therefore, they reason, technologically induced deindividuation should lead to greater uninhibited behavior in computer-mediated group decision processes.

The Siegel et al. (1986) team conducted three experiments using face-to-face communication, computer-mediated communication with anonymity, and computer-mediated communication with nonanonymity. The groups were asked to come to a consensus on different choice-dilemma problems. The experiment showed that the two computer-mediated groups experienced some inefficiency communicating as compared to face-to-face groups. The computer-mediated groups also participated more equally, were more uninhibited, and reached decisions that deviated further from initial individual preferences.

In a second experiment, the researchers lengthened the time for discussion to enable consensus. The results were consistent with findings in the first study. They conclude that deindividuation does occur and that submergence in a group, social anonymity, and the lowered salience of social controls or standards lead to feelings of loss of identity and uninhibited behavior.

This study provides further evidence that "submergence in a technology, and technologically-induced anonymity and weak social feedback might also lead to feelings of loss of identity and uninhibited behavior" (Siegel et al., 1986, p. 183). The researchers illustrate by noting that people who would never read someone's regular mail would not think twice about looking over the shoulder of a colleague who is reading e-mail. The researchers conclude by suggesting that deindividuation occurs due to exposure in the computing subculture which produces uninhibited behaviors affecting decision-making. The data show that people may respond differently in different communication settings and that computer-mediated communication's effect on organizational decision-making and problem-solving may be more complex than previously believed.

Some of the research has shown positive results of deindividuation and computer usage. Deindividuation in some studies has been found to elicit conformity to group norms. Spears, Lea, and Lee (1990) found that a greater polarization occurs in the direction of a group norm in deindividuated-group conditions as opposed to deindividuation-individual conditions.

Lea and Spears (1991) went on to explore the effects of deindividuation on computer-mediated communication and decision-making. They found that the technological features of electronic communication trigger psychological states and processes resulting in less normative influences on individuals and groups, as well as more deregulated and extreme behavior. The occurrence of uninhibited behavior, such as "flaming" and more polarized decisions by groups, shows a recurring theme. In the absence of social influences and contextual cues and because of the reduced impact of social norms and constraints, computer-mediated communication evidences some of the same conditions important for deindividuation.

Lea and Spears (1991) conducted an experiment based upon the social identity theory, which infers that individuals have different identities, both as unique individuals and as members of social groups. In their study, they sought to determine whether participants are deindividuated by virtue of being isolated and anonymous as opposed to being co-present with others.

Deindividuation was operationalized in the study by manipulating the subjects' physical locations and social anonymity. In the deindividuated condition, all were separated physically. In the individuated condition, participants were clearly visible to the other subjects. The findings showed that subjects in the deindividuated-group condition were more polarized in the direction of a group norm. The greater polarization was associated with exchange of significantly fewer words, shorter messages, and a significantly smaller proportion of remarks related to the topic.

The study also provided evidence that through deindividuation the participants' social identity became more salient than their individual identity because of anonymity within the group. Lea and Spears (1991) found some evidence that contrasted with similar studies. Deindividuation does not have to be thought of as a deregulated state associated with uninhibited behavior unless that is a prevailing group norm. The group norm predicts behavior, which may be either positive or negative. They also found that deindividuation is not necessarily contingent upon the physical co-presence of the group and was not necessarily associated with uninhibited behavior (Lea & Spears, 1991).

In an earlier study, Hiltz, Turoff, and Johnson (1989) also found support for the conclusion that deindividuation could be positive or negative depending upon the established group norm. They hypothesized that pen name conferences might demonstrate more disinhibited and deindividuated behavior than conferences in which comments were signed with the real name of the contributor. The pen name was used as a form of anonymity.

The researchers defined deindividuation as a "decreased reliance by individual group members on their own opinions and values, and increased conformity to group opinions and norms" (Hilt et al., 1989, p. 221). Therefore, deindividuated behavior is "going along with the group," which does not necessarily mean negative, irrational, or abnormal behavior. Deindividuation was also found to involve a decrease in the amount of self-consciousness and self-monitoring of behavior.

A similar study dealing with computer-mediated communication found no support for deindividuation. These researchers (Matheson & Zanna, 1988) do agree with others that computer-mediated communication draws attention away from one's self and the social context and toward communication tasks. In contrast to others, their conclusion suggests that relative to the face-to-face communication group, subjects using computer-mediated communication report significantly higher levels of private self-awareness, and marginally lower levels of public self-awareness.

A possible explanation is that low public self-aware individuals interacting with the computer may have felt fewer inhibitions and little concern about responding more negatively, which would be consistent with uninhibited behavior of computer users. In conclusion, the researchers believe that the use of computer-mediated communication involves a state of high private self-awareness rather than deindividuation.

In a final study, the Theory of Reasoned Action was compared with the Theory of Deindividuation in an effort to explain computer user behavior (Loch & Conger, 1996). The Theory of Reasoned Action has been used to describe ethical decision-making behavior and relates attitudes and social norms to individual behavioral intentions. The importance of the study by Loch and Conger (1996) is that evidence indicated that the Theory of Reasoned Action is useful for diverse decision-making situations but is inadequate to explain ethical behaviors involving the use of the computer.

Loch and Conger (1996) believe that privacy and ownership are two areas identified through their literature review as presenting consistent ethical dilemmas. The researchers defined privacy as the individual control over disclosure and use of information, which includes collection, accuracy, and distribution. Ownership was defined for research purposes as the rights of people to possess, use, and dispose of property.

In a proposed modification to the Theory of Reasoned Action, Loch and Conger (1996) introduce two factors that directly impact ethical attitude: deindividuation and computer literacy. The researchers hypothesize that attitudes are expected to relate to intentions to perform the computing acts. In computing ethics, social norms impact behavior, and the presence of a code would increase motivation to comply with social norms impacting intentions. Social norms are expected to relate to intentions to perform computing acts. An individual's self-image is expected to relate indirectly to intentions through attitude. Thus, deindividuated individuals, those experiencing alienating effects, could be expected to engage in antisocial behaviors. Deindividuation is expected to relate indirectly to intentions through attitude. As computer literacy increases and as the voluntary use of the computer increases, the extent of an individual's computer literacy is expected to relate indirectly to intentions through attitude. A final hypothesis states that men and women differ in their formation of ethical intentions.

Loch and Conger (1996) administered a questionnaire instrument over a 6-month period to graduate students in business policy classes in four urban universities. Two hundred fifty-three questionnaires were completed. The results support the contention that the Theory of Reasoned Action provides some explanatory power for ethical behavior intentions; however, modifications are necessary to obtain useful explanations of ethical computer decisions. A revised model shows that self-image, deindividuation, ethical attitude, computer literacy, and social norms all impact behavioral intentions.

This study provides important evidence that links attitudes and social norms. Evidence also supports the premise that both attitudes and social norms play an important role in determining an individual's intentions to perform computing acts relating to privacy and ownership. Moreover, men and women use different decision cues in forming intentions toward computing acts. Deindividuation, feeling of anonymity and distance, was found to be an important factor for some people in determining their computing behavior intentions.

Loch and Conger (1996) recommend that institutions take several actions. It is necessary to define acceptable computing behaviors for the environment and to define acceptable social norms. This would require policies and guidelines be developed or established to delineate social norms. They further recommend that individuals be provided education covering assumptions and attitudes toward ethical computing acts according to existing polices and guidelines.

Through the investigation and review of the existing body of literature, specific areas have been addressed. These areas consist of documentation of the societal influence created by computers, ethical literature, computer ethic research, legal materials, studies contributing to the development of computer ethics, insights from the business community, studies showing the effectiveness of computer ethics policies, and finally, behavioral models research.

Summary

As discussed previously, organizational leaders within higher education have a unique opportunity to help educate computer users to make prosocial choices when faced with ethical dilemmas. The literature supports the use of computer ethics instruction and computer ethics policies as effective measures in facilitating ethical conduct by computer users. Moreover, the body of research regarding the study of behavioral models, particularly the Theory of Deindividuation, indicates that an increased understanding and awareness of the underlying factors involved in unethical behavior are possible through the application of such theories.

The Theory of Deindividuation is well-suited for the development of a computer ethics policy and instructional plan because it can clarify and reveal user behavior. The Theory of Deindividuation identifies the presence of personal identity and social identity of an individual. Social identity may be promoted, and the computer makes this process much easier by assisting in the identification and connection of other individuals. As others are identified, personal responsibility for behavior becomes less significant and, for some, insignificant thereby deindividuating the individual. The computer is also a tool in minimizing social identity in favor of personal identity. The computer may remove the ability of others to evaluate and punish because computer users may conceal their identity or perceive that they are free from external influences. As a result the individual becomes deindividuated without identification and accountability.

Effective policies must be more than a list of rules. They must be written to have a positive and profound impact on computer user behavior. Applying the theory of deindividuation enables educators to uncover and reveal the motivational factors affecting user behavior. Armed with this understanding, they can take steps to encourage identification with higher ethical group standards and re-awaken and reinforce personal standards or convictions as well. Particular measures and guidelines may then be incorporated within the policy and implemented through the instructional plan, based upon deindividuation, to increase ethical behavior by computer users.

In light of the fundamental and theoretical concerns and issues raised previously, the review of literature does confirm a need for more research. Organizational leaders faced with ethical dilemmas are raising serious questions and seeking answers. To better equip educational leaders for addressing technology-induced ethical concerns, further research is necessary. Research is needed within the area of computer ethics instruction and more specifically computer ethics policies and their effectiveness.

Chapter III: Methodology

After examining the many and various ethical problems and issues caused by information technologies and their uses, the analysis of literature, and review of previous attempts to create a computer ethics policy (see Appendix D), the need for further research focusing on computer ethics policies and instructional needs in higher education is evident. A survey of community college administrators was undertaken by using a measuring instrument designed to confirm the theoretical assumptions that educational leaders are being faced with ethical dilemmas that demand solutions and that they need information enabling them to develop policies, procedures, and ethical instruction for computer users. System administrators were also asked for their response to a preliminary draft of an ethics policy and plan of action incorporating basic concepts of the Theory of Deindividuation.

As expected, responses resulting from the survey provided insight regarding the nature and extent of computer technology-induced ethical issues and concerns of key leaders within the North Carolina Community College System. Responses from the preliminary policy and plan hopefully enabled key leaders and system administrators to feel a sense of ownership in a final computer ethics policy that is presented in Chapter VI. In addition, some of the individual needs and diverse groups within the 58 community colleges that comprise the North Carolina Community College System are reflected in one final policy and plan.

The survey was in part designed to determine the perceptions of administrators regarding the fundamental concepts of the Theory of Deindividuation as they related to computer ethics or improving computer ethics on their campuses. The theory generally was explained to the administrators in a summary of the purpose of this research project that was sent to each of them at the time their participation in the study was requested. Specific questions contained on the survey instrument used in the study were designed to measure the extent that administrators perceived this type of behavior was present among computer users on their campuses and the value of the theory of the theory of deindividuation in explaining this behavior. The questions designed for this purpose did indicate the presence of deindividuated behavior among current computer users on the participants' campuses. This feedback helped shape potential preventative or intervention strategies that have been incorporated into the model computer ethics policy and instructional plan presented in Chapter VI.

There were a number of underlying assumptions that guided the development and administration of the survey instrument and interpretation of the results. First, it was proposed that few well thought-out policies, if any, exist within the 58 community colleges composing the North Carolina Community College System. A preliminary search of Internet web sites of each of the colleges suggested this was the case. Secondly, there were occurrences of unethical behavior or antisocial conduct being reported by community college instructors and lab attendants at the time of the study. A third assumption was that these occurrences were causing educational leaders to ask questions regarding measures to curtail unethical behavior and to search for answers.

It was believed that few precautions or measures have been implemented due to the presence of unanswered questions; of those few precautions that have been implemented, few have led to any measure of success. A further assumption was that educational leaders would be receptive to a body of research revealing some of the contributing factors associated with behavior that the Theory of Deindividuation provides and would welcome measures to effectively control behavior through a computer ethics policy and instructional plan.

Based upon the information acquired through the survey instrument and an accompanying response sheet, what was found in previous research and supporting literature, and scrutiny of existing computer ethics policies including the state of North Carolina's general computer policy aimed at all state employees, a model computer ethics policy more complete and appropriate for students, faculty, and staff within the North Carolina Community College System was created. The model policy is accompanied by recommendations on how it may be implemented. This includes suggestions for courses of instruction that relate to and incorporate theoretical principles of deindividuation. The proposed computer ethics policy should not only assist North Carolina Community College System administrators but should aid other educational leaders plagued by information technology concerns and issues.

Survey Participants

Survey participants consisted of system administrators from the 58 community colleges comprising the North Carolina Community College System. The director of the North Carolina Community College System Information Services, Steve Ijames, was consulted to determine the appropriate contact person at each of the colleges. Mr. Ijames recommended that system administrators would be able to provide the most useful insights regarding computer ethics on their campuses or would direct the survey to the most appropriate person at their college. System administrators are individuals responsible for the maintenance of the hardware and software, network systems, and computer labs. These individuals also provide technical support for all end users, and represent the college concerning all information systems or management information systems contacts that are made.

The community college system was selected based upon the unique needs of community college educational leaders. North Carolina was chosen based upon the apparent need for computer ethics policies or more effective ones, and the researcher's familiarity with current issues and concerns within the system.

A survey participant list contains the names of each participating community college, their location within North Carolina, and the name of each system administrator to be surveyed (see Appendix E). In the absence of the particular title of System Administrator or Primary System Administrator, individuals listed first in order of seniority were chosen as the contact person. This includes individuals with the titles of Director, Dean, Network Administrator, Assistant, and Assistant Vice President.

Design and Procedure

The mail questionnaire technique was implemented for this study. The self-administered mail questionnaire was selected due to the confidential nature of the instrument and potential to elicit more truthful responses. Each system administrator or contact person was mailed an introductory letter and research purpose summary in an attempt to get a commitment from potential participants prior to sending the survey instrument (see Appendix F). In the initial mailing, a postage-paid post card was included. Administrators were to check the appropriate box indicating a willingness or unwillingness to participate in the study. In addition, they were asked to select their preferred method of receiving the packet of research materials. Almost all selected e-mail and provided their e-mail addresses.

The second mailing consisted of a cover letter reiterating the purpose of the study, a list of the enclosed documents, and instructions for returning the completed survey and response sheet (see Appendix G). Non-respondents from the first mailing were also sent the packet in addition to those wishing to participate (see Appendix G). This was done to encourage and provide an additional opportunity for participation and to increase the overall sample size. Only one system administrator did not receive the packet due to their returning the initial post card and indicating that they did not want to participate in the study. E-mail was used for sending the packet to participants who had indicated this as a preference and for nonrespondents that had e-mail addresses available through their college's web site.

All system administrators were provided with a computer ethics assessment instrument, a working model of a computer ethics policy, a working model of an ethical instruction plan, and a policy and plan response sheet (see Appendix H). Participants were asked to provide an assessment of the current conditions of unethical behavior and computer infractions occurring on their individual campuses. Participants were next asked for their input and assessment of specific policy elements and implementation ideas after they had received the enclosed drafts of policy and plan models.

To improve the overall response rate, participants were provided with an appropriate FAX number, telephone numbers, and e-mail addresses (personal and through the college) of the researcher to return the materials. For additional questions, concerns, or a preference in returning the instrument in a different method, participants were also invited to contact the researcher.

All respondents were asked to return the completed instrument in a timely manner. After a prescribed amount of time of approximately two weeks, follow-up letters reminding participants of the survey were sent with an enclosed postage-paid envelope in case they were experiencing difficulties in e-mailing or sending the documents through a FAX machine (see Appendix G).

One week later, a follow-up e-mail was sent to determine if there were concerns or needs and if an additional copy of the questionnaire were needed. Additional contact with participants that had not returned the survey and response sheet was made through a friendly, follow-up phone call after an additional week.

Materials

The design of the research questions consisted primarily of a five-point Likert scale, ranging from strongly agree to strongly disagree, and covered the following subject areas. The questions focused on the presence of an existing policy, the occurrence of certain listed unethical behaviors by users, and preventative measures attempted. Topical areas also addressed the importance of communicating computer ethics, the need for a policy proscribing acceptable behavior, and input concerning what a policy should contain. A series of questions guided by the theory of deindividuation addressed the anonymous nature of computer usage, the ability to identify with other groups through the Internet, and related unethical behavior. A final question inquired whether respondents felt a computer ethics policy would reduce unethical behavior through the individuation, as opposed to the deindividuation, of users. Additional questions were open-ended providing opportunities to extract further qualitative data from participants.

As a final measure employed by the researcher, the survey instrument was pretested by several current system administrators to perfect the instrument, remove unwanted ambiguity in responses, and to improve clarity for increased understanding.

Chapter IV:
Results of College Administrator Survey

The overall importance of this study is based upon the premise that information obtained from previous literature related to computer ethics on college campuses and computer ethics policies, coupled with input from college administrators that are most involved with computer ethics needs, issues, and problems on their campuses, could assist in the development of a model computer ethics policy primarily designed for community colleges in the North Carolina Community College System. This policy would be accompanied by recommendations for implementing it that included educational elements. The policy and recommendations would be shaped in part from the perspective of deindividuation theory.

Purpose of the Survey

It is important to reiterate that the main purpose of the survey portion of the study was not to find data that represented the universe of community colleges, but to obtain useful input from system administrators within the North Carolina Community College System regarding computer-related ethical conditions on their campuses. A secondary purpose of the survey was to obtain useful input that focused upon participants' reactions to elements of a working version of the computer ethics policy and an accompanying instructional plan being developed and proposed by this study. This was presented to them along with the survey instrument.

The results obtained from the completed surveys and response sheets have provided a great deal of interesting and useful data that successfully met these survey objectives and contributed greatly to the proposed model policy and ethical instruction plan contained in Chapter VI. They also provide a more comprehensive understanding of the ethical issues and problems within the North Carolina Community College System and elsewhere. In addition, responses to certain key questions do indicate the presence of deindividuated behavior among computer users on college campuses within the research area.

Respondents

Twenty-four system administrators agreed to participate in the study out of the 58 invited. Eighteen Computer Ethics Assessment Surveys and 15 Ethical Policy and Instructional Response Sheets were completed and returned. Participants were asked to respond to each of the questions using a five-point Likert scale, ranging from strongly agree to strongly disagree. The results of the surveys and response sheets are examined below in light of the key research questions that guided this study.

Due to the small size of the sample and the limited number of completed survey questionnaires, in-depth statistical analyses beyond descriptive statistics were not possible. Frequencies, means, and standard deviations were calculated. Frequencies are contained within Tables 1 through 14. The means and standard deviations are shown in Tables 15 through 29 in Appendix H. The data derived from the descriptive statistics basically provide a qualitative as opposed to a quantitative analysis.

Administrators Perceptions of the Extent of Computer Ethics Problems on Their Campuses

The first basic research question stated in Chapter I and explored through the survey was the extent to which various unethical or antisocial behaviors are occurring in computer labs or elsewhere on the campuses of community colleges within the North Carolina system. As shown in Table 1, more than three quarters (77.78%) of the respondents either agreed or strongly agreed that sharing user access or passwords, stealing passwords, or unauthorized accessing of data was taking place on their campuses. One half of the respondents (50.00%) either agreed or strongly agreed that showing a lack of respect for the privacy and security of other users, data, or network systems was an issue. More than three quarters (88.89%) either agreed or strongly agreed that using computing resources for purposes other than those specified or originally intended was going on.

Of those who participated in the survey, a little under one half (44.45%) either agreed or strongly agreed, while over one half (55.55%) either disagreed or strongly disagreed that using computing resources for personal gain was taking place. More participants (77.78%) either agreed or strongly agreed that monopolizing resources (playing games), and wasting software, hardware, or supplies was occurring.

As Table 1 also indicates, most of those responding (88.89%) either disagreed or strongly disagreed that using computing resources to commit crimes, theft, or destruction of hardware and/or software is taking place. Responses were almost split, with 44.44% agreeing and 55.56% disagreeing or strongly disagreeing that engaging in software piracy, illegally copying of licensed software, or infringing upon software license agreements was an issue. The respondents generally disagreed (11.11%) or strongly disagreed (83.33%) that users were knowingly transmitting or creating computer viruses on their campuses. The majority of those responding (94.44%) either disagreed or strongly disagreed that users were intercepting transmitted information, hacking into networks and systems, or cracking codes either on campus or from another location.

Almost as many agreed or strongly agreed (44.44%) as disagreed or strongly disagreed (55.56%) that users were engaging in the displaying, downloading, and viewing of inappropriate, offensive or obscene materials on their campuses. Most participants (83.33%) either disagreed or strongly disagreed that engaging in the transmission of obscene, defamatory, harassing, offensive, annoying, or abusive e-mails was taking place. The majority of those responding (94.44%) either disagreed or strongly disagreed that users were misrepresenting the college on the Internet or falsifying their identity. The same number of those responding (94.44%) either disagreed or strongly disagreed that users are posting information on the Internet that violates the college's code of conduct.

Table 1
Administrators' perceptions of the frequency of non-ethical incidents that are occurring on North Carolina community college campuses

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
Sharing user access or passwords, stealing passwords, or unauthorized accessing data	n	3	11	0	4	0
	f	16.67%	61.11%	0.00%	22.22%	0.00%
Showing a lack of respect for the privacy and security of other users, data, or network system	n	2	7	0	9	0
	f	11.11%	38.89%	0.00%	50.00%	0.00%
Using computing resources for purposes other than those specified or originally intended	n	5	11	0	2	0
	f	27.78%	61.11%	0.00%	11.11%	0.00%
Using computing resources for personal gain	n	1	7	0	7	3
	f	5.56%	38.89%	0.00%	38.89%	16.67%
Monopolizing resources (playing games); wasting software, hardware, or supplies	n	2	12	0	4	0
	f	11.11%	66.67%	0.00%	22.22%	0.00%
Using computing resources to commit crimes; theft or destruction of hardware and/or software	n	0	2	0	5	11
	f	0.00%	11.11%	0.00%	27.78%	61.11%
Engaging in software piracy, illegally copying of licensed software, or infringing upon software license agreements	n	0	8	0	7	3
	f	0.00%	44.44%	0.00%	38.89%	16.67%
Knowingly transmitting or creating computer viruses	n	0	1	0	2	15
	f	0.00%	5.56%	0.00%	11.11%	83.33%

Intercepting transmitted information, hacking into networks and systems, or cracking codes either on campus or from another location	n	0	1	0	7	10
	f	0.00%	5.56%	0.00%	38.89%	55.56%
Engaging in the displaying, downloading, and viewing of inappropriate, offensive or obscene materials	n	1	7	0	9	1
	f	5.56%	38.89%	0.00%	50.00%	5.56%
Engaging in the transmission of obscene, defamatory, harassing, offensive, annoying, or abusive e-mails	n	0	3	0	10	5
	f	0.00%	16.67%	0.00%	55.56%	27.78%
Misrepresenting the college on the Internet or falsifying their identity	n	0	0	1	3	14
	f	0.00%	0.00%	5.56%	16.67%	77.78%
Posting information on the Internet that violates the college code of conduct	n	0	0	1	3	14
	f	0.00%	0.00%	5.56%	16.67%	77.78%

Means also were calculated for each of the variables dealing with the extent that specific computer ethics problems existed on the administrators' college campuses. It was discovered through responses to one question contained in the survey that all but two of the respondents had some type of existing computer ethics policy at their college. Although sample size prevented determination of statistically significant differences, the responses of those administrators who had computer ethics policies were compared with those who did not. The two respondents whose colleges did not have an existing policy appeared to be experiencing higher occurrences of unethical behavior and computer use infractions than participants with an existing policy.

In response to an open-ended question that invited comments about inappropriate uses of computers at their colleges, the respondents, as a whole, mentioned the following in no particular order: e-mailing friends, family and other nonbusiness contacts; software theft, particularly Microsoft Office CD's; excessive student use of chat rooms; banging on equipment, hitting keyboards, and spilling coffee in keyboards; campus server misuse for personal use; student installation of personal software on college equipment; and games and chat programs being played during classes.

The respondents were asked about what steps or precautions had been taken to resolve ethical problems and their effectiveness. The responses of those who responded to this open-ended question included: established a firewall, developed an acceptable computer use policy, and monitored student use of the network; our college has acceptable use policy that students must agree to as well as faculty, and most labs have assistants; have implemented college-wide, acceptable use policy; posted signs and no food in lab; due to lack of IS personnel and administration's lack of awareness, very little is done to resolve problems; using software and hardware to lock computers and lock classrooms; no measures or precautions; in public access areas, software is used to protect the system (Fortress), and classrooms have a standard configuration that can be reloaded if necessary; network usage rules have been established and must be read before a user ID is given to a student, and accounts can be locked for misuse while severe violations are dealt with under the Student Code of Conduct by the Dean of Student Services; all students must scan all diskettes before using Open Lab computers; they must sign in and out, and students sign an Open Lab Policy agreement outlining prohibited actions each semester.

Growth of Computer Ethics Issues

A number of variables in the measuring instrument were an attempt to determine whether system administrators felt that computer technology-related ethical issues have increased on their campuses and if so, why and how the Internet usage has impacted these issues. As shown in Table 2, almost three quarters (72.72%) either agreed or strongly agreed with the statement that ethical problems had increased since their campuses provided connection to a local area network and Internet as opposed to providing just stand-alone PCs and general computer lab use. However, the respondents unanimously agreed or strongly agreed that student use of computers and the Internet have had a positive impact on their colleges. Finally, only a third (33.33%) either agreed or strongly agreed and one half disagreed or strongly disagreed with the statement that student uses of computer chat rooms have created safety issues or concerns for their colleges.

Table 2
Increase of technology-related ethical issues and impact of Internet usage

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
4. Ethical problems have increased since our campus provided connection to a local area network and Internet as opposed to providing just stand-alone PCs and general computer lab use.	n	3	10	0	5	0
	f	16.67%	55.56%	0.00%	27.78%	0.00%
6. Student use of computers and the Internet have had a positive impact on our college.	n	9	9	0	0	0
	f	50.00%	50.00%	0.00%	0.00%	0.00%
7. Student uses of computer chat rooms have created safety issues or concerns for our college.	n	1	5	3	7	2
	f	5.56%	27.78%	16.67%	38.89%	11.11%

Perceived Need for and Communication of a Computer Use Policy

Another important area of questioning sought to determine how many community colleges within the system have a computer ethics policy at the current time or feel that a policy is an important consideration. As shown in Table 3, most of the participants (83.33%) either agreed or strongly agreed that the ethical use of computers was becoming a critical issue that needs to be addressed at their colleges. Contrary to what was expected, a majority of those surveyed (88.89%) had a policy of some sort.

Table 3
Colleges with an existing policy and importance of having a policy

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
5. Ethical use of computers is becoming a critical issue that needs to be addressed at our college.	n	2	13	1	2	0
	f	11.11%	72.22%	5.56%	11.11%	0.00%
13. My college has an existing computer ethics policy for all computer users (acceptable use policy, or similar wording).	n	6	10	0	2	0
	f	33.33%	55.56%	0.00%	11.11%	0.00%

Another fundamental research question from Chapter I that guided the survey focused on the extent that community college administrators believe a computer ethics policy should be aligned with the mission and purpose of higher education or the particular mission of their educational institutions. As shown in Table 4, all participants either strongly agreed (44.44%) or agreed (55.56%) that a computer ethics policy was important for the protection of the mission and purpose of their colleges. Almost three-quarters of the participants (73.34%) either agreed or strongly agreed that it was appropriate for a computer ethics policy to open with the college's mission statement while only 20.00% disagreed.

Table 4
Alignment between mission of a college and a computer ethics policy

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongl Disagre
9. A computer ethics policy is important for the protection of the mission and purpose of our college.	n	8	10	0	0	
	f	44.44%	55.56%	0.00%	0.00%	0.00
1. It is appropriate for a computer ethics policy to open with the college's mission statement.	n	4	7	1	3	
	f	26.67%	46.67%	6.66%	20.00%	0.00

Need for Computer Ethics Instruction and Enforcement of Policies

As shown in Table 5, almost three quarters (73.34%) either agreed or strongly agreed that an ethics component should be included in all computer classes at their colleges, while the remaining responses were split between no opinion (13.33%) and disagree (13.33%). In addition, more respondents (40.00%) either agreed or strongly agreed rather than disagreed (20.00%) that instructors at their colleges would be receptive to spending class time teaching ethics; however, a high number of respondents (40.00%) indicated no opinion.

Table 5
Perception of the need for an ethical component within college computer classes

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
17. Instructors at my college would be receptive to spending class time teaching ethics.	n	1	5	6	3	0
	f	6.67%	33.33%	40.00%	20.00%	0.00%
18. An ethics component should be included in all computer classes at my college.	n	3	8	2	2	0
	f	20.00%	53.34%	13.33%	13.33%	0.00%

Another basic research question that the study attempted to answer was concerned with how participants might enforce a computer policy and asked whether this should apply equally to students, faculty, and staff. While the respondents were given the opportunity to provide written comments regarding this, they did not do so. On the other hand, as Table 6 indicates, almost three quarters (72.22%) expressed disagreement with the idea that faculty and staff rarely contribute to computer-related ethical problems. Only 16.67% felt that this group was not involved. All participants either strongly agreed (80.00%) or agreed (20.00%) that a computer ethics policy should be applicable to all users rather than just students. Nearly three quarters (73.33%) either agreed or strongly agreed that faculty and staff should be bound to the policy although not required to sign a contract.

Table 6
Applicability of a computer ethics policy to all users (faculty, staff, and students)

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
8. Unlike students, the faculty and staff rarely contribute to ethical problems relating to computing resources at my college.	n	1	2	2	11	2
	f	5.56%	11.11%	11.11%	61.11%	11.11%
6. A computer ethics policy should be applicable to all users rather than just students.	n	12	3	0	0	0
	f	80.00%	20.00%	0.00%	0.00%	0.00%
12. Faculty and staff at my college should be bound to the policy although not required to sign a contract.	n	5	6	0	3	1
	f	33.33%	40.00%	0.00%	20.00%	6.67%

Application of the Theory of Deindividuation

Since this study was in part an effort to examine computer ethics problems and solutions from the perspective of the Theory of Deindividuation, a number of survey questions addressed this. The primary focus of the survey was to secure input from college administrators that would be helpful in the development of a computer ethics policy that would meet the growing needs in this respect on their own and other college campuses. However, by including a number of research questions on the survey instrument that generally asked participants to assess the extent of "deindividuation" behavior among computer users on their campuses and their perceptions of the applicability of the basic theory for the development of a computer ethics policy, it was hoped that a better model policy and ethical instructions related to it could be created. At the same time responses to these questions might further explain or reinforce what has discovered and asserted in previous research related to the Theory of Deindividuation—that the theory could be used to explain and predict underlying computer user behavior in terms of motivational factors. The theory is one of the few behavioral theories identified by scholars as useful in understanding motivational forces that facilitate computer user behavior and takes into consideration both personal and social identity.

As shown in Table 7, over 40% agreed that computer users' anonymity on the Internet may have led to a number of unethical computer usage incidents at their college and an additional third were not certain, while less than a quarter disagreed. Almost two thirds (61.11%) of the participants either disagreed or strongly disagreed with the notion that computer users at their colleges use computers in ways that they normally would not because there is less likelihood of getting caught.

As Table 7 reveals, only 16.67% agreed that the Internet increases the occurrence of unethical and antisocial behavior because computer users in their labs can easily identify others exhibiting similar unethical and/or antisocial behaviors. The same percentage of participants registered no opinion, while two thirds (66.66%) disagreed or strongly disagreed with the idea.

In contrast, more agreed (73.33%) than disagreed (20.00%) that many users understand ethical conduct, but feel they can escape detection at their colleges. All respondents either strongly agreed (20.00%) or agreed (80.00%) that computer users at their colleges would behave more ethically if they perceived that they could be monitored during general computer usage in the labs. Once again respondents were unanimous in agreement that computer users at their colleges would behave more ethically if they perceived that they could be monitored during specific Internet usage in the labs. It is possible that participants reacted more objectively to questions 10 and 11, and provided a more subjective, behavioral interpretation of the remaining questions as shown in Table 7.

Table 7
Theory of Deindividuation usage to explain ethical behavior of computer users on community college campuses

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
10. The fact that computer users can remain anonymous on the Internet may have led to a number of unethical computer usage incidents at our college.	n	1	7	6	3	1
	f	5.56%	38.89%	33.33%	16.67%	5.56%
11. Computer users at our college use computers in ways that they would normally not because there is less likelihood of getting caught.	n	0	6	1	8	3
	f	0.00%	33.33%	5.56%	44.44%	16.67%
12. The Internet increases the occurrence of unethical and antisocial behavior because computer users in our labs can easily identify others exhibiting similar unethical and/or antisocial behaviors.	n	0	3	3	11	1
	f	0.00%	16.67%	16.67%	61.11%	5.56%
20. Many users understand ethical conduct, but feel they can escape detection at my college.	n	1	10	1	2	1
	f	6.67%	66.66%	6.67%	13.33%	20.00%
24. Computer users at my college would behave more ethically if they perceived that they could be monitored during computer usage in our labs.	n	3	12	0	0	0
	f	20.00%	80.00%	0.00%	0.00%	0.00%
25. Computer users at my college would behave more ethically if they perceived that they could be monitored during Internet usage in our labs.	n	3	12	0	0	0
	f	20.00%	80.00%	0.00%	0.00%	0.00%

Another basic question posed in Chapter I was whether the Theory of Deindividuation is a useful perspective to have when developing computer ethics policies, procedures, and accompanying instruction. As shown in Table 8, a little over one half (55.55%) either agreed or strongly agreed that a computer ethics policy and ethics instruction at their colleges would increase ethical and prosocial behavior because users would identify with appropriate behavior. More than four out of five (86.66%) either strongly agreed or agreed that explaining what constitutes unethical behavior appears to be best conveyed through listing examples in the policy. Over one half

(66.67%) of those responding agreed, while less than one tenth (6.67%) disagreed and almost one third (26.66%) had no opinion about the connection between student anonymity and unethical behavior.

Table 8
Utilization of the Theory of Deindividuation for developing computer ethics policies and instruction

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
15. A computer ethics policy and ethics instruction at our college would increase ethical and prosocial behavior because users would identify with appropriate behavior.	n	2	8	5	2	1
	f	11.11%	44.44%	27.78%	11.11%	5.56%
7. Explaining what constitutes unethical behavior appears to be best conveyed through listing examples in the policy.	n	4	9	1	1	0
	f	26.66%	60.00%	6.67%	6.67%	0.00%
26. There is a connection between student anonymity and unethical behavior at my college; the presence of a computer ethics policy and signed contract would reduce their anonymity.	n	1	9	4	1	0
	f	6.67%	60.00%	26.66%	6.67%	0.00%

A related research question posed in Chapter I was concerned with whether elements of the Theory of Deindividuation can be embedded in the computer policies, procedures, and instruction themselves. As shown in Table 9, most (86.66%) agreed that requiring students to sign a contract would make them feel more identified and cause them to behave more ethically at their colleges. Over one half (66.67%) agreed that the presence of a computer ethics policy and signed contract would reduce student anonymity, and 55.55% agreed that a computer ethics policy and ethics instruction would increase ethical conduct by helping users identify with appropriate behavior.

Table 9
Potential of elements of the Theory of Deindividuation to be embedded in computer policies and instruction

Question		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
15. A computer ethics policy and ethics instruction at our college would increase ethical and prosocial behavior because users would identify with appropriate behavior.	n	2	8	5	2	1
	f	11.11%	44.44%	27.78%	11.11%	5.56%
22. The fact that students sign a contract would make them feel more identified and cause them to behave more ethically at my college.	n	1	12	1	1	0
	f	6.67%	79.99%	6.67%	6.67%	0.00%
26. There is a connection between student anonymity and unethical behavior at my college; the presence of a computer ethics policy and signed contract would reduce their anonymity.	n	1	9	4	1	0
	f	6.67%	60.00%	26.66%	6.67%	0.00%

Model Computer Ethics Policy and Ethical Instruction Plan

System administrators also were asked for their input concerning the components that should be included in a computer ethics policy. The following constitutes the study participants' recommendations and evaluations of a preliminary draft of a policy and accompanying instructional plan presented to them for their inspection. As shown in Table 10, most (80.00%) agreed that the policy purpose appeared to need no additional information or explanation. Thirteen out of the 15 respondents (86.67%) either agreed or strongly agreed that the components listed in the Guidelines for Appropriate Computing Behavior cover all the major ethical issue areas and that no additional sections are needed. The same number (86.67%) either strongly agreed or agreed that explaining what constitutes unethical behavior appears to be best conveyed through listing examples in the policy. A little under one half of those responding either agreed (13.33%) or strongly agreed (33.34%) that the liability section of the proposed policy was needed, but would require revisions for their colleges.

Table 10

Participants' input concerning the components to be included in a computer ethics policy

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
2. The policy purpose appears to need no additional information or explanation.	n	0	12	1	2	0
	f	0.00%	80.00%	6.67%	13.33%	0.00%
4. Components listed in the Guidelines for Appropriate Computing Behavior cover all the major ethical issue areas and no additional sections are needed.	n	1	12	2	0	0
	f	6.67%	80.00%	13.33%	0.00%	0.00%
7. Explaining what constitutes unethical behavior appears to be best conveyed through listing examples in the policy.	n	4	9	1	1	0
	f	26.67%	60.00%	6.66%	6.67%	0.00%
8. The liability section is needed, but would require revisions for my college.	n	2	5	6	2	0
	f	13.33%	33.34%	40.00%	13.33%	0.00%

In response to two open-ended questions that asked for additional information regarding the proposed policy, the respondents provided the following suggestions: add the sentence "Unacceptable use is prohibited and is grounds for loss of computing privileges, as well as prosecution under federal, state, and local law"; state that authorized personnel are the only individuals to install any hardware or software on machines; the first sentence of the computer ethics policy should encompass faculty and staff as well as students; and the contract should be for all users with a penalty imposed for probation or firing of employees; state that faculty, staff, or students should have a copy of the agreement for freeware or shareware on file for auditing purposes; and indicate that any statement regarding legal action has been reviewed and approved by the college attorney.

The remainder of the policy and plan response sheet focused upon several research assumptions posed in Chapter I. These assumptions not only addressed key issues designed to increase ethical behavior but also provided evaluation that relates to the usage the Theory of Deindividuation framework that was used in this study.

Table 11 shows the first set of response sheet questions relating to the research assumption focusing on the use of a student contract. Of the respondents, 80.00% either agreed or strongly agreed that the student contract is a necessary component in order to make students accountable for their behavior at their colleges. Most (73.33%) either disagreed or strongly disagreed with the statement that student signatures on a contract probably would have very little impact on their behavior at their colleges. More agreed (46.67%) than disagreed (20.00%) that the signed student contract should be considered a legal document and would reduce liability issues at their colleges. Most (86.66%) agreed that students' signatures on a contract would make them feel more identified and cause them to behave more ethically at their colleges. One half of those responding (53.34%) either disagreed or strongly disagreed with the statement that students should be given an access number or other means of tracking because the contract alone is insufficient to reduce unethical behavior.

Table 11

Necessity and benefits of a student contract component within the computer ethics policy

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
10. The student contract is a necessary component in order to make students accountable for their behavior at my college.	n	5	7		3	0
	f	33.33%	46.67%	0.00%	20.00%	0.00%
11. Student signatures on a contract probably would have very little impact on their behavior at my college.	n	0	3	1	9	2
	f	0.00%	20.00%	6.67%	60.00%	13.33%
21. The signed student contract should be considered a legal document and would reduce liability issues at my college.	n	1	6	5	3	0
	f	6.67%	40.00%	33.33%	20.00%	0.00%
22. The fact that students sign a contract would make them feel more identified and cause them to behave more ethically at my college.	n	1	12	1	1	0
	f	6.67%	79.99%	6.67%	6.67%	0.00%

23. Students should be given an access number or other means of tracking, because the contract alone is insufficient to reduce unethical behavior.	n	0	5	2	7	1
	f	0.00%	33.33%	13.33%	46.67%	6.67%

The next research assumption addressed the perceived effectiveness of a computer ethics policy and thus indirectly explored whether a policy in itself could serve as deterrent as the Theory of Deindividuation seemed to suggest. As shown in Table 12, one half of those responding (53.33%) agreed, while only 33.33% disagreed that a computer ethics policy will most likely reduce or eliminate unethical behavior at their colleges.

Table 12

Effectiveness of a computer ethics policy in support of the Theory of Deindividuation

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
13. A computer ethics policy will most likely reduce or eliminate unethical behavior at my college.	n	0	8	2	5	0
	f	0.00%	53.33%	13.34%	33.33%	0.00%

Table 13 shows the results of the research assumption concerning the evaluation of the ethical instructional plan. More respondents either agreed or strongly agreed (33.33%) than disagreed (20.00%) that the ethical instruction plan appears relevant and necessary to increase ethical behavior at their colleges; however, almost one half (46.67%) had no opinion. Most of those responding (73.33%) disagreed that students probably would not understand the computer ethics policy without the instructional plan. Over one half of those responding (53.33%) disagreed or strongly disagreed that students probably would not abide by a computer ethics policy without computer ethics instruction. Not surprisingly, most (66.66%) of those responding disagreed or strongly disagreed with the statement that many computer users act unethically at their colleges simply because they do understand how to behave ethically.

Table 13

Evaluation of the ethical instructional plan

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
14. The ethical instruction plan appears relevant and necessary to increase ethical behavior at my college.	n	2	3	7	3	0
	f	13.33%	20.00%	46.67%	20.00%	0.00%
15. Students probably would not understand the computer ethics policy without the instructional plan.	n	1	2	1	11	0
	f	6.67%	13.33%	6.67%	73.33%	0.00%
16. Students probably would not abide by a computer ethics policy without computer ethics instruction.	n	1	5	1	7	1
	f	6.67%	33.33%	6.67%	46.66%	6.67%
19. Many computer users act unethically at my college simply because they do understand how to behave ethically.	n	1	1	3	9	1
	f	6.67%	6.67%	20.00%	59.99%	6.67%

The next research assumption addressed whether system administrators felt that a policy and plan would reduce unethical behavior and would benefit their colleges. Of the respondents, most (86.66%) either agreed or strongly agreed that a computer ethics emphasis similar to the model policy and instructional plan would benefit their colleges.

Table 14

Potential of the computer ethics policy and instructional plan to reduce unethical behavior and benefit the colleges

Variable		Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree
27. A computer ethics emphasis similar to the model policy and instructional plan would benefit my college.	n	2	11	1	1	0
	f	13.33%	73.33%	6.67%	6.67%	0.00%

As a final component to the response sheet asking for additional input, suggestions, and recommendations through an open-ended question yielded the following responses: include a section on data security, particularly plagiarism; to keep in mind that what is unethical to one individual may not be unethical to another individual; and a computer ethics class is a great idea, however, identifying and discussing ethical issues might inform students how to intentionally inflict harm.

In conclusion, evidence provided by this study did indicate the presence of a substantial number of unethical incidents occurring on campuses within the North Carolina Community College System. Based upon responses to the survey instrument, insights regarding the nature and extent of these incidents, as well as ethical issues and concerns of key leaders within the system were documented. Additional valuable data provided by participants in this study confirmed that behavior described by deindividuation theorists was applicable to computer user behavior.

As stated previously, the primary purpose of the survey portion of this study was to obtain useful input from system administrators within the North Carolina Community College System regarding computer-related ethical issues and concerns. A secondary purpose of the survey was to acquire valuable insight based upon reactions of the participants to elements of a computer ethics policy and instructional plan being developed and proposed by this study. These results are discussed and conclusions and implications presented in Chapter V and they were applied to the model policy and instructional plan presented in Chapter VI.

Chapter V: Discussion

All parts of society increasingly have become dependent upon computers, including the education field and its institutions of higher learning. However, technological advancements in and applications of computers in the educational context often have progressed faster than consideration of their impact upon cultural norms and values or the development of ethical standards governing the use of computers. A wide variety of ethical issues that have emerged in the computer field generally, many unique to the Internet and its use, are particularly problematic in the educational setting. The basic dilemma confronting leaders in higher education remains balancing the need for freedom of information access while accommodating the various conflicting social values of diverse communities.

The results of the survey of college administrators conducted in this study not only confirm that this is the case, but point to the need for effective computer ethics policies that are appropriate for the needs of students, faculty, and staff on college campuses. The focus of this study was the community college, rather than other types of educational institutions. The growing importance of community colleges and the opportunity they have to reach a larger, more diverse student population makes this educational platform worthy of special investigation.

As discussed in Chapter I, the need for computer ethics policies and ethical instruction may be more critical at the community college level than at other institutions of higher learning. The typical community college student received little if any computer instruction at the public school level, and in many cases enters the community college for the purpose of learning about information technology. The community college also services GED and adult high school students for individuals that have left the public school system. In many cases, these students are considered "high risk" lacking adequate guidance and supervision.

The community college has an opportunity to reach individuals who may not decide to attend institutions of higher education. Many businesses and industries provide training to their employees through community college continuing education programs. In addition, these individuals may encounter ethical dilemmas and situations to a greater degree with minimal ethical instruction.

A final reason that the community college serves a critical role is due to its service to the community. This may include ethical instruction for unemployed persons, migrant workers, and senior citizens. As a result of such diversity, the community college has an opportunity to reach groups of people needing computer ethics instruction beyond the scope of other institutions.

This study concentrated on the North Carolina Community College System, leaders at colleges within this system, and their perceptions of the need for computer ethics policies or improvements in existing ones on their college campuses. The North Carolina Community College System appears to be very representative of community college systems nationally in terms of population, enrollment, impact, emphasis, and community. In addition, preliminary research indicated that the North Carolina community college leaders are committed to responding to the demands of an ever-changing information technology environment.

In order to develop a model computer ethics policy and plan to implement it, this study also was concerned with the individual behavior of the computer user. One behavioral theory that offers a particularly promising framework for developing college computer ethics policies and ethical instruction is the Theory of Deindividuation (Festinger, Pepitone, & Newcomb, 1952; Zimbardo, 1969). As discussed in Chapter II, the basic hypothesis of this theory suggests that when individuals are submerged within a group they become anonymous and lose conscious personality. This feeling of being unseen and not personally identifiable enables individuals to express primitive feelings and impulses, and possibly unethical behavior. The Internet and other uses of computers seem to prompt this form of identification and individual behavior. Moreover, recent studies have confirmed that users exhibit behaviors similar to deindividuated behaviors when submerged in a computer as when submerged in a group.

The results of the survey presented in Chapter IV offer further insights for educational leaders about current computer ethics problems and issues and viable solutions to them. The findings suggest that using new theoretical perspectives may be helpful in the effort to create effective computer ethics policies and to reduce or eliminate unethical behavior.

This research also provides a glimpse of the extent of computer infractions and unethical conduct that currently exists within higher education. In addition, the results of the survey of community college administrators and their reactions to a model policy and accompanying instructional plan led to a more refined model and plan that are presented in Chapter VI. This policy and plan should serve educational leaders of community colleges and other educational institutions that are seeking practical solutions for reducing or eliminating unethical computer use behavior on their campuses.

In this chapter, survey findings are discussed in light of the key research questions that guided this study. Recommendations based on the results and discussion of them are offered to community college leaders and others. In the discussion that follows, the fundamental research questions and findings related to it are briefly restated. This is followed by an interpretation of what the particular findings mean. Next, the findings from this study are compared with previous studies related to computer ethics and how this study contributes to the existing body of knowledge. The discussion then concentrates on what the findings from this study imply with regard to prevailing theoretical models, and concludes with what should be included in a policy and how it should be structured.

Research Questions and Main Findings

The survey of community college administrators first explored the extent to which various unethical or antisocial incidents were occurring in computer labs or elsewhere on the campuses of community colleges within the North Carolina Community College System. Between one half and three quarters of the participants indicated that access or passwords issues, privacy and security concerns, harassment, and unintended use of computing resources were a problem at their campuses.

In contrast, according to almost all the study participants, more serious issues such as theft, computer viruses, hacking, and misrepresenting or falsifying identities were found to be uncommon at their colleges. In between these two extremes, issues such as personal gain, illegally copying of software, and displaying and downloading of inappropriate materials were a problem for half of those surveyed.

The survey provided college administrators with an opportunity to provide more insights concerning additional inappropriate uses of computers at their colleges. Those surveyed stated that noncollege related uses of e-mail and chatting were a concern as well as inappropriate uses of software and hardware. Participants were also asked what steps or precautions had been taken to resolve ethical problems. Responses ranged from doing nothing to developing policies and posting signs. Additional suggestions included software and/or hardware to eliminate and reduce the effects of unethical behavior.

System administrators also were questioned as to whether they thought that computer technology-related ethical issues had increased and if Internet accesses had contributed to this. Of those surveyed, almost three-quarters felt that ethical problems had increased since they had networked their computers even though all agreed that the Internet has had a positive impact on their campuses. Contrary to what the researcher anticipated, only a third expressed concern about student uses of computer chat rooms.

An additional finding not anticipated was the high percentage of those surveyed that had some form of existing computer ethics policy. This is particularly interesting considering almost all of them indicated that the ethical use of computers was becoming a critical issue that needed to be addressed at their colleges. This would suggest that their current policies need to be modified or replaced by policies and plans of implementation that can more effectively deal with computer ethics complexities that are being experienced on their campuses.

In response to questioning on the subject, it seems clear that community college administrators believe a computer ethics policy should be aligned with the particular mission of their educational institution. All of those surveyed felt that a computer ethics policy was important for the protection of the overall mission and purpose of their colleges, while almost three quarters felt it was appropriate for a computer ethics policy to open with the college's mission statement.

Almost three quarters of the respondents in the survey believed that an ethics component should be included in all computer classes at their colleges. However, when asked if instructors would be receptive to spending class time teaching ethics, 40% of the respondents answered "no opinion" as if reluctant to evaluate instructor response to such a request or uncertain as to whether instructors would be willing. Nearly three quarters of the participants were not reluctant, though, in admitting that faculty and staff contributed to computer-related ethical problems on their campuses. In addition, everyone agreed that a computer ethics policy should be applicable to all users rather than just students.

Responses to questioning that was concerned with behavior explained by the Theory of Deindividuation further suggested that it is a useful perspective to have when developing computer ethics policies, procedures, and accompanying instruction. The idea that the Theory of Deindividuation can be embedded in some way within computer policies, procedures, and instruction seemed to be at least generally confirmed.

Over 40% agreed that computer users' anonymity on the Internet may have led to a number of unethical computer incidents at their college and an additional one third of those surveyed were not certain. Surprisingly, only one third of the participants thought that users at their colleges operate computers in ways that they normally would not because there is less likelihood of getting caught. Even fewer confirmed the connection between identifying outside groups on the Internet and increases in unethical behavior. While not disproving the concept of deindividuation, the tendency for the administrators to perceive that their computer labs did not foster behavior described by deindividuation theorists did not lend credence to the theory.

A finding that did support the concept of deindividuation was the admission by almost three quarters of the participants that they felt many users understand ethical conduct but believe they can escape detection at their colleges. In addition, the respondents all disclosed that computer users at their college would behave more ethically if they perceived that they could be monitored during computer usage in the labs. They also agreed that monitored Internet usage in the labs would facilitate ethical conduct.

Overall, the results of the study did suggest that the Theory of Deindividuation is a useful perspective to have when developing computer ethics policies and instruction. A little over half of those surveyed agreed that a policy and instruction would enable users to identify with appropriate behavior thereby increasing ethical conduct, and more than four out of five felt that listing examples in the policy is beneficial. Supporting the use of the theory, over half of those surveyed thought there was a definite connection between student anonymity and unethical behavior. Most of the respondents also agreed that requiring students to sign a contract would make them feel more identified thereby reducing anonymity and increasing ethical consciousness and appropriate conduct.

As part of their review of the model computer ethics policy included with the survey, system administrators were asked for their input concerning components that should be included in such a computer ethics policy. Most of those surveyed felt that the policy's purpose statement and behavioral guidelines were complete without need of further modifications. However, a little under half suggested that the liability section of the proposed policy, while needed, required revisions suited to their colleges. When asked what revisions were necessary, the respondents most often focused on additional penalties such as reminding users that they may suffer the loss of computing privileges, potential prosecution under federal, state, and local laws, and the possible probation or firing of employees. The study participants also expressed an interest in addressing faculty and staff more within the body of the policy and signed contract.

Generally, the results of the survey supported some of the main assumptions that guided this study as a whole. A more detailed, clearer computer ethics policy that contains examples of ethical behavior; addresses the computer ethics needs of students, faculty, and staff; and is integrated with the overall mission of the college, might better meet the needs of community college leaders trying to cope with computer ethics problems and issues on their campuses. Such a policy should have provisions for accountability such as the signing of a contract by all computer users. A well-developed and implemented policy that includes this and other features that acknowledge and deal with the behavior described by deindividuation theorists would go a long way toward reducing or eliminating unethical behavior on community college and other college campuses. Half of those responding expressed confidence that a computer ethics policy could reduce or eliminate unethical behavior at their college.

The participants were also asked to evaluate the ethical instruction plan that was included in the survey packet. More agreed than disagreed that the ethical instruction plan was necessary to increase ethical behavior, however, almost half had no opinion. Some respondents may have been supportive of the idea of computer ethics instruction tied to a computer ethics policy and plan of implementation, but may have not been certain if the particular course of instruction presented to them was the best way to accomplish this. Most of those surveyed also felt that students would understand the policy without instruction, although this does not preclude the need for such instruction to gain compliance to such a policy. One participant elaborated on this issue by stating that a computer ethics class was a great idea, but expressed concern that the identification and discussion of ethical issues might inform students how to intentionally inflict harm.

Interpretation and Comparison to Past Research Findings

The following section of the discussion will concentrate upon interpretation of the research findings in light of the major purposes of this study. In addition, three areas are given deeper analysis and scrutiny: a) The extent of unethical incidents occurring on the campuses of community colleges within North Carolina, and the degree to which educational leaders are faced with these concerns and issues; b) Whether and in what specific ways the results of the survey of administrators support the need of having a computer ethics policy (or a more effective policy) and ethical instruction to solve many of the major dilemmas resulting from unethical behavior; c) The practicality and usefulness of the Theory of Deindividuation as a framework for creating and implementing ethical policies and plans. The research findings in this study are then considered in light of the existing body of knowledge related to computer ethics cited earlier in Chapter II, the literature review section.

The college administrators questioned in this study reported that there were more incidents of less severe computer infractions than extreme ones. Less severe problems such as software piracy or illegal copying of licensed software was found to occur in 45% of the cases, and more severe issues such as hacking into networks occurred in just 6% of the cases. This is consistent with the findings of Pulliam (1994) who found that 47% of those surveyed listed less severe ethical issues, such as software piracy as occurring while more severe issues, such as hacking were reported by only 16% of the participants in that study. Betts (1995) also found that 47% of those surveyed admitted to copying commercial software.

Despite the fact that between half and three quarters of the participants in the survey of community college administrators indicated that less severe computer infractions as cited above were occurring, all but two indicated that they already had a computer ethics policy. This would seem to suggest that these existing policies or procedures or the means by which they were implemented, explained, or taught were ineffective in eliminating unethical behavior. The lack of more severe infractions could be in part attributed to typical composition of the population of community colleges. They tend to serve older adults, many of whom are not as computer literate or sophisticated with the methods unethical computer users sometimes use to inflict serious damage. Moreover, some research studies suggest that people tend to become more ethical and moral in their decision-making processes as they age (Josephson, 1992; Parker, Swope & Baker, 1990; Paradice, 1990).

Although only two of the respondents in the survey indicated that they did not have computer ethics policies on their campuses, the reported incidences of unethical behavior at these colleges were higher than for those that stated their college had a policy. Although this was not a statistically significant finding, it does hint that a computer ethics policy does reduce occurrences of unethical behavior. Hegarty and Sims (1979) similarly found that policies could act as a deterrent to unethical behavior. Vitell and Davis (1990) also noted the positive impact of codes of ethics on ethical behavior, and Day and Day (1996) found that students preferred a computer use policy to regulate and outline ethical behavior rather than censorship.

The community college administrators surveyed in this study were asked to report the incidence of specific types of unethical behavior that have been discussed in computer ethics literature. Most of these dealt with misuse of computer software. However, the respondents also identified other computer ethics problem areas that are of concern, namely stealing CDs and physically abusing equipment.

The results of this survey of community college administrators suggested that at some colleges steps or precautions had been taken to resolve ethical problems. Again, most of the participants stated that some form of policy had been implemented at their campuses. Some participants reported that students had to read and agree to the policy before user IDs were given. Others stated that users must sign a policy agreement in addition to signing in and out in the labs.

However, when directly asked to respond to a survey question about what steps or precautions had been taken to deal with unethical behavior, the second most common response was that no measures or precautions had been taken. Those who responded this way seemed to believe that existing computer ethics policies were having minimal effect and/or that administrative awareness of the extent and importance of the problem had been missing.

An important aspect of this study sought to determine if system administrators thought that computer technology-related ethical issues have increased and if Internet access has contributed. Even though almost three quarters responded that ethical problems have increased since their colleges had connected to the Internet, there was a lack of concern regarding chat rooms and bulletin boards. This may be understandable given the nature of chat software. It is almost impossible to determine what has been said after terminating the program, because all potentially incriminating evidence, not intentionally saved by the user, is lost. Another plausible explanation could be the lack of usage at the community college level by students thereby decreasing the attention or concern by system administrators.

Prior to conducting this study, all of the North Carolina system community colleges' web sites had been searched and no policies or evidence of any were found. It is quite probable that although many of these colleges have computer ethics policies, they may vary considerably in purpose, nature, and effectiveness. Some could be very detailed while others simply involve a sign posted in a lab. The fact that they are not contained at the colleges' web sites suggests that they are not being communicated as extensively as the general scope of the problem seems to merit. It is worth pointing out again that even though many of the community colleges examined in this study did have computer ethics policies, most of the study participants thought ethical issues needed to be addressed or addressed more fully. This would support the need not only for better policies but also for computer ethics instruction and other plans of action that would better insure that such policies worked.

Almost three quarters of those surveyed felt that an ethics component should be included in all computer classes at their college. This is consistent with the findings of Pulliam (1994) who found that 70% of those surveyed felt that including computer ethics in the curriculum is of extreme importance. Sheel and Collins (1997) also agree that ethics needs to be an integral component in all technical courses, and Petrick (1992) found that ethics should be institutionalized.

Regardless of the belief that an ethics component should be included, there was a seeming lack of strong interest in ethical instruction. Most of those surveyed within this study even suggested that students would understand ethical concepts without providing any ethical guidance. Perhaps these administrators had received very little instruction in computer ethics themselves and thus were unfamiliar with the nature of such instruction and underappreciative of its relevance in dealing with practical computer ethics problems. They may also have been uncertain about how such instruction could be carried out within the structure of their particular colleges and programs or how computer ethics instruction related to a computer ethics policy. Moreover, their responses may have merely reflected general disinterest in the particular course of instruction posed to them in the survey.

DeLoughry (1988) confirms that there is a failure on the part of many colleges and universities to teach their computer science students about the social and ethical responsibilities they will face as professionals. Magner (1989) confirms that while 63% believe that the curriculum should include a mandatory ethics course, only 26% reported that their school currently required one. Walden and Gordon (1988) also found that respondents in their study overwhelmingly agreed that ethics should be taught in courses; however, only 47% of them required their students to take such courses. Furthermore, of the classes that were taught, 68% of the instructors devoted less than 10% of their course time to ethics instruction.

Again, a major purpose of this study examined the practicality and usefulness of the Theory of Deindividuation as an underlying perspective for dealing with computer ethics problems, particularly at college institutions. The basic constructs of the theory seem to have potential for guiding the development of computer ethics policies, procedures, and accompanying instruction.

One question in particular was critical in terms of testing the idea of deindividuation on system administrators. Over 40% agreed that computer users' anonymity on the Internet may have led to a number of unethical computer incidents at their college and an additional one third of those surveyed were not certain. Only 4 of the participants disagreed entirely. It is possible that some of the participants may have been confused about what the term deindividuation meant, although a definition was provided initially in the research summary that was sent in the first mailing to the administrators. On the other hand, two additional questions concerning deindividuation generated disappointing results. Again, it was surprising to find that only one third of the participants felt that computer users at their college operate computers in ways that they normally would not because there is less likelihood of getting caught. The wording in this question may have been confusing to the respondents. It is possible that they may have had misconceptions about the word "normally" or were uncertain what constituted "normal" individual computer behavior. They also may have thought that their particular computer labs or atmosphere of the campuses made "getting caught" more likely, thus making the question somewhat irrelevant.

Only 3 of the participants agreed that the Internet increases the occurrence of unethical behavior because computer users in their labs can easily identify others exhibiting similar unethical behaviors. Once again, the participants may not have understood the wording or meaning of the question. The phrase "easily identify others exhibiting similar unethical and/or antisocial behaviors" could have been interpreted as just other individuals within a computer lab rather than those that the user might have observed or interacted with via the Internet.

In contrast, almost three quarters of the participants indicated that many computer users understand ethical conduct, but feel they can escape detection at their colleges. In addition, the disclosure by all respondents that computer users at their college would behave more ethically if they perceived that they could be monitored during computer usage in the labs suggests that applying the notion of deindividuation to encourage ethical behavior can be accomplished. They also agreed that monitored Internet usage in the labs would facilitate ethical conduct. As a final affirmation of the applicability of the Theory of Deindividuation, only one of the participants disagreed that there is a connection between student anonymity and unethical behavior, and that a policy would solve this problem by reducing their anonymity.

These findings are consistent with the findings of Zimbardo (1969). He found that deindividuated unethical behaviors are more likely to be expressed when there is a loss of personal identity. Kiesler (1986) found that participants communicating by a computer feel a greater sense of anonymity and detect less individuality in others. Kiesler, Siegel, and McGuire (1984) suggest that being submerged in the computer is very much as when individuals are submerged in a group. Siegel, Dubrovsky, Kiesler, and McGuire (1986) also found evidence for a "technologically-induced" anonymity. Finally, Lea and Spears (1991) found that through deindividuation an individual's social identity becomes more prominent than their individual identity because of anonymity within the group.

Based upon the findings of this study, there appears to be support for using the

Theory of Deindividuation for policy design, implementation, and ethical instruction. Strong support was also established for embedding premises of the theory within the policies, procedures, and instruction themselves.

The survey respondents generally seemed to verify, at least indirectly, that encouraging identification with appropriate behavior would help resolve the computer ethics problems on their campuses. A little over half indicated that a policy and instruction could serve this purpose. Furthermore, most respondents agreed that enabling students to identify with ethical behavior is best conveyed through listing examples. Presenting behavior for users to identify with enables students to deindividuate, but in a positive, specific way. Deindividuation is not always a negative phenomenon, but is dependent upon established group norms. Thus, if a policy demonstrated a group norm that facilitated ethical behavior and users identified with this behavior, users would become more ethical in their computing conduct.

This finding is consistent with Spears, Lea, and Lee's (1990) study that revealed that a greater polarization occurs in the direction of a group norm in deindividuated group conditions. Lea and Spears (1991) further confirmed that the group norm predicts behavior, which may be either positive or negative. Hiltz, Turoff, and Johnson (1989) in an earlier study also found support for the connection between deindividuation and established group norms. Finally, Loch and Conger (1996) recommend policies and guidelines be developed or established to delineate social norms, and to provide education covering assumptions and attitudes toward ethical computing acts in view of existing polices and guidelines.

Another means of applying the theory to policy development concerns the use of a student contract. Only one participant disagreed that students' signatures on a contract would make them feel more identified, therefore increasing ethical behavior. The user contract portion of a computer ethics policy "individuates" computer users making them aware of the fact that they can be identified. This increases their accountability. Nearly a majority of the study participants indicated that the contract was necessary to make students accountable. A little over half of the participants even suggested that a student contract alone would be sufficient to reduce unethical behavior.

The high percentage in favor of student signatures seems to indicate that system administrators would view a student contract as valid and believe students should be treated as adults and be held responsible for their actions. Since the typical community college student is older, employed, and has a family, this perspective is especially understandable. The fact that the maturity level of the community college student typically is much higher may explain the hesitancy on the part of many of the study participants to support the idea of computer ethics instruction related to the policy. The community college administrators may have believed not only that such instruction was less necessary but that this type of student was less in need of or more difficult to deal with in matters of behavior and discipline.

A few of the participants did allude to their rationale for not responding enthusiastically to the idea of ethical instruction. They thought that what might be unethical to one individual may not be unethical to another. Basically they did not want to interfere with the personal belief systems of the students. One participant expressed concern that by identifying and discussing ethical issues, some students might be encouraged or informed about how to intentionally inflict harm. While these concerns are understandable, it should not be cause for prohibiting ethical instruction. There are generally agreed-upon truths and standards of behavior set by the community college that are necessary to maintain college policies regardless of the like or dislike of faculty, staff, or students.

Contributions of the Survey Research

The findings from this survey, although limited in scope, contribute to the ongoing demand for scholarly research on computer ethics issues and policies in the context of higher education. These findings do elucidate and verify some of the pressing concerns facing educational leaders due to information technology. In particular, computer ethics problems do exist extensively on many community college campuses; however, more severe problems such as hacking, theft, and virus-spreading are not currently great problems.

The survey data did correct the false assumption that few computer ethics policies exist within the North Carolina Community College System. The participating colleges have varying forms of computer ethics policies. However, they are apparently limited in their effectiveness. Most of the participants reported unethical computing behavior regardless of the presence of a policy.

The survey findings indicate a need for better policies that provide more detail, plans to make them work, and ethical instruction and guidance. Current system administrators and educational leaders may not be aware of the extent of their problems or how to effectively address them. They may also be underestimating the potential and overall importance of computer ethics education.

Essentially, education concerning computer ethics is just as significant as education focusing upon any other element critical to the needs of community members within society. Most educational leaders agree that demands placed upon people in our contemporary society make it almost impossible to function without the knowledge of how to use computers. One may add that, given the importance of computer knowledge and skills and the potential power that can be wielded by the computer user, it is imperative that individuals learn how to use computers ethically. The ethical component should not be viewed as a separate option, but rather as a critical facet of computing knowledge, expertise, and skill.

Limitations of the Survey

There are several limitations of the survey portion of this study worth noting. The most noticeable limitation relates to the small sample size. The beginning population of the research area was 58, and of that amount only 24 agreed to participate in the study. The sample size was restricted even further when only 18 out of the 24 chose to complete the survey. Of those 18 participants, 3 who completed the survey did not complete and return the response sheet. As a result, only 18 surveys and 15 response sheets were usable for data analysis.

The Theory of Deindividuation may possibly help explain why a number of administrators did not participate in the study. All of the system administrators within North Carolina received an invitation to participate in the study. They may have perceived that they were part of the group of administrators and as such may have felt deindividuated. They may have believed that their lack of participation would not be readily identifiable. Perhaps the usage of a reward by the researcher or the implied threat of punishment by a supervisor could have had the effect of individuating them toward participation in the study. An additional explanation for a lack of response could have been that the system administrators were reluctant to admit the ethical problems and issues experienced on their campuses due to possible self-incrimination and identification.

The small sample size made it impractical to conduct various statistical tests in the study. Had the sample size been more significant, a factor analysis could have been possible. A more meaningful analysis would have resulted in a clearer understanding of significant relationships among key variables in the study. For example, certain types of computer ethics problems that the administrators as a collective reported as existent on their campuses may have clustered together. In addition, a multiple regression analysis may have been used to determine whether specific variables incorporated in the study were good predictors of other phenomena. For example, the presence or absence of a computer ethics policy on the community college campuses could have been predictive of a higher degree of ethical or unethical conduct.

The second limitation was the researcher's lack of anticipation that many colleges had existing computer ethics policies. As noted earlier, all web sites of the 58 community colleges were examined for any evidence of a policy or ethical instruction. Even though no evidence of existing policies was found through web sites and other means, it seems fairly clear from the responses of the community college administrators that these existing policies were very limited in scope and/or inadequately communicated or applied. However, anticipation that they existed in some form at many of the colleges would have led to the inclusion of questioning about them within the survey instrument. In anticipation that policies existed, questions could have been posed regarding specific conditions under which they came into existence. It also would have been interesting to find out how long they have had a policy, who was involved in creating it, what specific elements were contained in it and how it had been promoted.

A third limitation relating to the higher than anticipated number of existing policies was that the concept of a computer ethics policy might not have been operationally defined well for the respondents. Although many participants stated in an open-ended response they had developed a computer ethics policy, anticipation that these policies existed could have resulted in requesting administrators to send a copy of their policy when they returned their completed questionnaires. A copy of a policy that was provided by one community college is contained in Appendix J.

Finally, more questions could have addressed the ethical instruction plan, or possibly alternative plans, to provide clarity concerning the system administrators' perceptions of this seemingly important aspect of alleviating computer ethics problems on college campuses. The evidence is inconclusive as to exactly why respondents in the study did not favor the ethical instruction plan incorporated into the survey design. In addition, it would have been helpful to determine more specifically if they currently had any computer ethics instruction in place or other measures for dealing with computer ethics problems at their colleges.

The findings from this survey, despite the limitations and small sample size, are still an important and relatively unique contribution to this study. The survey did accomplish the basic objectives it was designed to fulfill and provided the necessary data and ideas needed to develop a more useful model computer ethics policy and instructional plan.

The information from the study proved to be very valuable. The key implications gleaned from the survey were instrumental in the refinement of the computer ethics policy, instructional plan, and contributed to the related recommendations that will be discussed in detail in Chapter VI. The resulting model and plan would have been unrepresentative of the North Carolina Community College System as a whole without the valuable insight and wisdom provided by system administrators through the use of the survey instrument utilized in this study.

Chapter VI: Model Computer Ethics Policy and Instructional Plan

With regard to the findings from previous research, supporting literature, and feedback provided by community college administrators acquired through a survey instrument and response sheet, the purpose of this chapter is to present a refined model of a computer ethics policy and instructional plan for students, faculty, and staff within the North Carolina Community College System. Recommendations are included to assist educational leaders and system administrators in the implementation of such a policy and plan. Additional recommendations are suggested to assist and help direct scholars interested in contributing to computer ethics research.

Rationale for a Computer Ethics Policy

This chapter begins with a review of related literature highlighting what various scholars have suggested were important policy development guidelines and essential content areas that should be included in any computer ethics policy. Next, information and sources reviewed by the researcher, including numerous examples of policies are discussed. These contributed to the development of the proposed policy model presented in this chapter. The unique computer ethics and policy needs of community colleges, particularly those within North Carolina, are a particular focal point. In addition, this discussion will demonstrate how this proposed model policy is applicable to all colleges and universities, and how it may provide guidance and assistance to educational leaders interested in adopting a new policy or improving an existing one.

The final component of this section presents the model computer ethics policy. The policy itself is contained in Appendix M. How basic theoretical principles of deindividuation are incorporated into the policy is explained. This model policy is not only based on what was discovered about computer ethics and computer ethics policies through secondary sources, but was shaped by insights and input from system administrators within the North Carolina Community College System. Changes made to an original draft of the policy presented to system administrators for their reactions are discussed.

The second segment of this chapter affirms the importance of ethical instruction. It is contended that educational instruction concerned with ethical use of information technology is critical to the success of this model policy or other computer ethics policies. Recommendations derived from supporting literature about the importance of ethical education, effective teaching approaches, suggested courses, and possible limitations are also discussed. Proposed content of ethical instruction that may be included as a module integrated within all existing curriculum computer courses is presented.

To further assist educators interested in computer ethics instruction a small sample of additional materials available through various resources on the Internet is supplied (see Appendix K). A wide assortment of such resources, in addition to the small sample, may be found on the Internet for those interested in pursuing computer ethics instruction within their courses. Materials such as course syllabi, case studies, group projects, reading lists, research documentation, and much more are easily found through a general search.

The third section of this chapter offers implementation suggestions and guidelines for a computer ethics policy and ethical instruction. These include procedures found by researchers to be most effective to communicate policies and procedures on college for deindividuation. These researchers (Matheson & Zanna, 1988) do agree with others that computer-mediated communication draws attention away from one's self and the social context and toward communication tasks. In contrast to others, their conclusion suggests that relative to the face-to-face communication group, subjects using computer-mediated communication report significantly higher levels of private self-awareness, and marginally lower levels of public self-awareness.

A possible explanation is that low public self-aware individuals interacting with the computer may have felt fewer inhibitions and little concern about responding more negatively, which would be consistent with uninhibited behavior of computer users. In conclusion, the researchers believe that the use of computer-mediated communication involves a state of high private self-awareness rather than deindividuation.

In a final study, the Theory of Reasoned Action was compared with the Theory of Deindividuation in an effort to explain computer user behavior (Loch & Conger, 1996). The Theory of Reasoned Action has been used to describe ethical decision-making behavior and relates attitudes and social norms to individual behavioral intentions. The importance of the study by Loch and Conger (1996) is that evidence indicated that the Theory of Reasoned Action is useful for diverse decision-making situations but is inadequate to explain ethical behaviors involving the use of the computer.

Loch and Conger (1996) believe that privacy and ownership are two areas identified through their literature review as presenting consistent ethical dilemmas. The researchers defined privacy as the individual control over disclosure and use of information, which includes collection, accuracy, and distribution. Ownership was defined for research purposes as the rights of people to possess, use, and dispose of campuses. Further recommendations deal with ways to insure that computer ethics issues and means of addressing them are an ongoing concern for community college administrators, faculty, staff, and students. Additional considerations are the role of campus culture in terms of computer ethics, and the interested parties to be included in the creation and implementation stages of policy and instruction development.

The final portion of this chapter focuses upon the need for further research regarding computer ethics policies, plans, and procedures. The contributions of this study are examined in light of implications for scholars and educational leaders. Directions for future research are suggested. This chapter concludes with a summary that points to the future of computer ethics issues in the higher education context.

Proposed Policy

The literature review in Chapter II provides sound recommendations and advice concerning effective strategies for developing computer ethics policies. Kallman (1992) argues that policies should place responsibility for ethical action on the individual but also include provisions for the college to take action when necessary. Anderson (1996) cautions, however, that policies should not be a list of do's and don'ts because such a negative approach may provide an incentive for a hacker to strike or prompt other forms of rebellious behavior.

Policy development guidelines.

There are several content areas that scholars have deemed necessary to consider in policy development. Some of these include protection of academic freedom, privacy issues, and compliance with software license agreements (Brown, Colter, & Short, 1994). Day and Schrum (1995) offer advice for policy content specifically geared toward usage of the Internet. They recommend that a policy begin with a definition of the Internet; the rules, or Netiquette, of the Internet; what constitutes objectionable material; the difference between Internet rights, privileges, and penalties; and repercussions for misuse of the Internet.

Petersen and Hodges (1997) propose additional recommendations for policy development. Effective computer ethics policies should establish the context by including a preamble or mission statement. Next, the scope of resources should be defined with an identification of who has access. It is also important to define computer user expectations and list examples of inappropriate behavior. Computer users should also be provided the procedure for reporting violations and information showing potential consequences of computer use infractions.

Anderson (1996) also offers recommendations for the primary components of a sound computer ethics policy. The policy should clearly differentiate between right and wrong, be consistent, and provide distribution of the keys to access particular data only when necessary. He further adds that policies should define acceptable use that relates to the overall mission and objectives of the organization, clearly state the institutional position, state college rules, and define penalties and punishments. Finally, he suggests that policies should differentiate between unauthorized and authorized use, define misuses, and provide specific rules that apply just to the Internet.

Sample policies examined. In addition to the literature reviewed that recommended effective strategies and development guidelines, 50 university and college computer policies were examined in terms of content, coverage, and structure (see Appendix L). These policies were selected based primarily upon two criteria. First, all of the major public universities within North Carolina were selected. It was believed that any particular issues relevant to North Carolina might be included within these policies. North Carolina universities also were examined to determine if any common themes existed among them that should also be included in community college policies.

Policies also were selected for review based upon the national recognition that particular universities and community colleges had for effective computer policies. This information was provided through the use of general searches on the Internet that retrieved links to sites where policies could be found.

A list of common core components and sections were compiled and a basic consensus was derived for pertinent areas to be included within the original draft of the computer ethics policy developed in this study. Appendix L indicates some of the fundamental policy components that were either included or missing within the sample of policies that was examined. As a result of examining policies from universities and community colleges nationwide, this original draft of a model policy could easily be applied within any community college or university. When presented to community college administrators in North Carolina to obtain their input, no mention was made of specific clubs, groups, or organizations unique to any particular community college or other institution. This made the drafted model policy and responses to it more transferable to other institutions.

Particular needs of community colleges. While common themes were extracted, several key issues were addressed due to the unique needs and opportunities of community college leaders as discussed in Chapter I. The community college serves a more diverse group of students; this factor contributed to substantially more wording in the model policy than many of the policies examined. The examples indicating inappropriate computer use behavior as listed within the model computer ethics policy had to speak to a more diverse population.

The proposed policy also had to anticipate technological changes, future advances, and potential for expansion given the dynamic nature of the community college system. The overall structure of the policy was designed specifically for future modifications and was written to effectively incorporate additions, alterations, and deletions with minimal time, effort, and money. The recommendation presented later in this chapter of a committee was suggested for the purpose of keeping the model policy up-to-date, and to anticipate changes and growth in information technology.

Symbolic role of North Carolina community colleges. The particular needs within the North Carolina system of community colleges for a better computer ethics policy played a symbolic role in the development of the model policy. This system is very comparable to other states in student diversity, responsiveness to community needs, workforce preparation, university transition, high school completion, and adaptation to changing technology. A second consideration in the creation of a model policy was the apparent need for effective computer ethics policies within North Carolina community colleges based on the preliminary search for and evaluation of existing policies.

Application of Theory of Deindividuation. The Theory of Deindividuation was used as a framework for developing the content of the policy. As stated earlier, the core components of the model computer ethics policy were derived based upon a consensus of pertinent areas to be addressed. While these general topics were based upon the sample of policies examined in the study, the actual wording and decision to include behavioral examples was based upon the application of this theory.

As discussed earlier, the Theory of Deindividuation is one of the few behavioral theories identified by scholars as useful in understanding behavior and takes into consideration both personal and social identity. Moreover, research has shown that deindividuation is not always negative, but rather is based upon the established group norms with which an individual identifies. The listed examples in the model policy contained in Appendix M address behavior that computer users should not engage in. This serves the purpose of establishing a group norm with which they should identify. Thus, appropriate behavior is implied for all computing activities rather than just the listed examples, and users are encouraged to conform to what they perceive as the established group norms as defined by the policy.

A second contribution from the Theory of Deindividuation was that it could be used to address the issue of accountability. Research based upon the theory establishes the fact that a contractual agreement with consequences of personal liability, accountability, and identification reduces the negative effects of deindividuation. As a result the likelihood that individuals will coexist within boundaries of established group norms when they may be identified is greatly increased. The model computer ethics policy proposed in this study contains a user contract for the purpose of making users aware that they can be identified and singled out.

System administrator input and policy changes. A major aspect of this study was to gain valuable input and insight from North Carolina Community College System administrators, including their reactions to the working draft of the policy and an accompanying instructional plan. System administrators were asked to evaluate the various parts of the policy and to suggest any additional sections or components they felt should be included.

The model policy (see Appendix M) begins with the mission statement of the college. The majority of those responding to the survey agreed with this concept. The computer ethics literature and institutional policies reviewed also confirmed that the policy should be in line with the mission of the university or college. The next section in the policy discusses the policy purpose and why it is important as it relates to and maintains the mission of the institution. Once again, inclusion of this information was based upon the literature and the draft of the model policy examined and confirmed by the system administrators.

The second section comprises the largest component of the policy and addresses the guidelines for appropriate behavior. The subsections consist of the following: a) Integrity and Accuracy, b) Copyright and Licensing, c) Privacy, d) Damages and Material Usage, and e) Internet and Electronic Mail. These five areas were included based upon the consensus of the policies examined. They also were critical issue areas identified by scholars and practitioners interested in computer ethics and referred to in Chapter II.

Examples were listed within these subsections to fully explain behavior that was deemed inappropriate or unethical. The more effective and lucid policies that were examined in this study and literature concerned with policy creation and implementation, both suggested that good examples of appropriate or inappropriate ethical behavior better enables students and others to identify with ethical concepts or standards. Again, the Theory of Deindividuation also suggests that clear identification with appropriate behavior reduces the negative effects of deindividuation. Community college system administrators who participated in the survey portion of the study agreed that examples were the most effective way to communicate appropriate computing behavior, and agreed with the way they were presented in the model policy draft they examined.

The survey of system administrators revealed that the liability section of the model policy draft was in need of a few minor revisions. The review of existing policies revealed that there is considerable variation in existing state and local laws that influence university and college policies. The survey of college system administrators further confirmed this. As a result, a small section containing fairly generic wording with regard to liability was created. This made it more easily adaptable to the unique needs of other colleges and universities.

The final section of the policy consists of a contract. The literature reviewed indicated that the more effective policies contained contracts making users more responsible and identifiable in case legal remedies were sought. The Theory of Deindividuation also contributed to the rationale for including a contract, suggesting that such a document would identify users and make them more accountable. Initially this contract was intended for students. However, the majority of the participants in the study agreed that this should apply to all those interested in utilizing computing resources at the college.

Community college system administrators also were asked for additional contributions to the policy draft. One individual suggested that the sentence "Unacceptable use is prohibited and is grounds for loss of computing privileges, as well as prosecution under federal, state, and local law" be added. Another participant felt that the policy should state that authorized personnel are the only individuals who should be allowed to install hardware or software on machines. Yet another felt that the first sentence of the computer ethics policy should spell out its relevance for faculty and staff as well as students. A participant offered the opinion that the contract should be for all users with a stiff penalty imposed for violations. Another response indicated that faculty, staff or students should have a copy of the agreement for freeware or shareware on file for auditing purposes. Finally, it was suggested that a notation be included that any statement regarding legal action had already been reviewed and approved by the college attorney.

Based upon this valuable feedback and input from system administrators, a number of changes were made to the original draft of the policy contained in Appendix H. The first sentence of the policy purpose was expanded to include faculty and staff in addition to the students. The last sentence of the policy purpose was rewritten to include local laws as well as state and federal ones. Another adjustment was a line inserted in the second sentence of the copyright and licensing section. This line reads "all licensing agreements must be kept on file for auditing purposes."

Two specific revisions were made to the liability section as a result of the survey. The third sentence was appended with the statement "and potential prosecution under federal, state, and local laws." The last sentence in that section was also added. This sentence reads, "Statements regarding legal action have been reviewed and approved by the college attorney." The final revision was in the contract portion of the policy, which was changed from "Student Contract" to "User Contract."

The final version of the computer ethics policy contained in Appendix M reflects the valuable feedback and insightful contributions from system administrators within the North Carolina Community College System. Based upon this, the policy is more appropriate for the community college setting, particularly those within North Carolina, although it is certainly applicable to other institutions of higher education.

Proposed Instructional Plans

Ethics education is a critical component for the overall success of a computer ethics policy and to encourage ethical behavior in general. Unfortunately, the findings in this study suggest that many educators think they should not be responsible for the ethical and moral development of others, but should simply teach objective concepts and facts. Many educational leaders and administrators also hesitate to develop and institutionalize ethics education. Some have suggested that if computer ethics were a required course at institutions, it would be legitimized and professors or others would be more anxious to teach it (DeLoughry, 1988).

Importance of ethical instruction. Some system administrators questioned in this study felt that ethical instruction was unnecessary. Some even suggested that it would possibly make the situation worse. It is interesting to note that at the same time many indicated high occurrences of unethical behavior that could potentially be avoided by better educating computer users.

As argued in this paper, teaching the ethical aspects of computer use is just as important as teaching basic computer concepts and skills. Many educational institutions have found this to be the case and have implemented various types of activities designed to empower their students for ethical actions (see Appendix K).

Day and Day (1996) offer recommendations for computer ethics education. They insist that ethics should be real and practical rather than abstract and ideal. Murphy and Boatright (1994) advise that education should assist students to become more alert at discovering moral issues, should teach them to reason ethical issues, and should clarify moral aspirations.

Some educators and administrative leaders debate whether to provide ethical instruction within all computer courses or to offer just one. Many scholars believe that ethics education is best taught and learned throughout the curriculum with a variety of ethics activities rather than compartmentalized within one course (Pollack, 1994; Schulze & Grodzinsky, 1997; Riser & Gotterbarn, 1996).

In view of the findings of this study and related literature reviewed, it appears that ethics instruction would be more practical as a module incorporated within all computer courses. Moreover, by not delegating or restricting ethics instruction to one class several obstacles may be avoided. First, ethical instruction would best serve the purpose it is intended by allowing as many students as possible to be exposed to it. If an ethical course were required, it probably would be required for only certain majors. It is argued that all users should receive ethical instruction concerning the use of computers regardless of their field of study. The most effective way to reach all or most students is through integration of ethical concepts within all computer courses. Faculty and staff, on the other hand, could receive computer ethics instruction through workshops, seminars, or professional development activities at their particular institutions.

A second potential obstacle relates to compartmentalization. In some cases, when concepts are confined to a certain area, students fail to see how they integrate and fit together with other seemingly unrelated topics. If ethics instruction is compartmentalized and people follow suit, they are more likely to feel that ethics does not relate to a majority of computer uses or does not relate to them or their particular interests at all. Through the integration and incorporation of ethical concepts within computer modules inserted in many courses of instruction, it is hoped that computer users will begin to see how ethical concepts relate to all issues involved in computer use and apply to their specific fields or areas of interest.

Teaching approaches in computer ethics. A computer ethics policy is only the first step in the process of instilling ethical behavior on college campuses. After implementing of the policy, ethical instruction should be viewed as an ongoing process. It is only fair to educate computer users concerning the policy if they are to be held accountable for the precepts listed in that document. Educational efforts will help insure that computer users on college campuses understand specific matters of accountability, why they are important, and what consequences result from being unaccountable.

In addition to educating students, Latimore (1997) emphasizes that one of the most important factors for successful ethical education is for faculty to promote and maintain a climate consistent with high ethical standards. Couger (1989) recommends that teaching approaches should begin with a dictionary definition of ethics relating to computer use. This should be reinforced by role-playing to determine how ethics would fit in real-life scenarios and be followed by encouraging students to personalize the topic within group discussions.

Sivin and Bialo (1992) also offer advice for effective teaching strategies. They begin with guidelines for an instructional unit. First, instructors should begin by introducing key concepts and definitions relating to computer ethics. Second, they need to include relevant historical and legal information related to ethical use of computers. Next, they should provide examples of ethical issues that may be of personal relevance to students. They suggest involving student participation through assigned readings, computer-based activities, writing assignments, role-playing, and classroom discussion. An additional activity to elicit student participation is the use of mock trials of cases involving unethical use of technology. A meaningful follow-up could include having students conduct surveys of other students' attitudes concerning computer ethics issues.

Suggested ethics instruction modules. System administrators in this study were asked to assess a proposed ethical instruction plan. While many believed that computer ethics instruction was an unnecessary aspect of effectively implementing a policy, this finding is in contrast to other research studies discussed in this chapter. Although it has been argued that ethical instruction, when it has been implemented, has been somewhat lacking in institutions of higher education, many scholars do agree that ethical instruction of some sort is necessary, beneficial, and important (DeLoughry, 1988; Summers & Markusen, 1992; Walden & Gordon, 1988; Ward, Ward & Wilson, 1996; Sivin & Bialo, 1992; Kizza, 1996).

Therefore, it is highly recommended that educational leaders interested in promoting ethical conduct by computer users develop and employ a plan for computer ethics instruction. The ethical instruction plan reviewed by the community college system administrators in this study generated no suggestions concerning necessary revisions; therefore, it has been recommended as a possible means of computer ethics instruction for all community colleges. It is presented in Appendix M.

This proposed ethical instructional plan incorporates a number of critical factors that were highlighted in the literature. The primary focus of ethics education should be to empower computer users to make sound ethical judgements based upon the weighing of social and moral choices when faced with ethical dilemmas. No policy can predict all the potential ethical situations that may occur, nor provide the correct answer for all ethical questions. This demands that users receive the skills and education necessary for effective decision-making. More important still, individuals must receive instruction and insight to assist them in identifying when moral and ethical issues are present.

Effective teaching strategies as identified in the literature should include a wide variety of learning formats and platforms. The primary focus should be on actively engaging students in the learning process and assisting computer users in attaching personal meaning and relevance for the various topics discussed.

The particular needs of the community college setting make this particular format of delivery, as suggested in the proposed instructional plan, very appropriate. The community college tends to cater to a diverse student population, and the variety of cases used in the instructional plan cover a vast assortment of groups, situations, and dilemmas. In addition, the cases are more reflective of the workplace and community in which these particular computer users will reside and interact. This particular plan also provides the flexibility to cover issues as needed and in as much or as little detail as necessary. Factors may be added or deleted as the situation warrants; activities may be modified to cover current topics, situations, or needs. This flexibility and adaptability fits nicely into the community college environment which tends to be more dynamic and reflective of community needs, technological advancements, and future trends.

The module approach also is flexible enough to fit the diverse curricula, departments, and schools that are found at the community college level. This approach tends to be an effective means by which ethical instruction may be inserted easily within a wide variety of courses without disrupting general course competencies. This approach would enable the module to fit as an independent unit transferable to various topics and time frames within the semester. Each module would be independent without the need for prerequisite modules. Moreover, this independence would ultimately enable more comprehensive analyses of the topics based upon timeliness and need.

Each component of the policy is broken down into 16 modules, and is based upon the 16-week semester term. By covering one topic per week, it is premised that the various topics may be covered in more depth. The most effective method of delivery would be to address each topic at some point during each class meeting. The discussion of cases and topic coverage could be either at the beginning or ending of each class, with additional references made during the class period showing the practical application of policy precepts.

The proposed instructional plan covers each of the core behavioral competencies as addressed in the computer ethics policy. As discussed earlier, the Theory of Deindividuation is used as a framework for building a composite group norm. This group norm is established by the policy and thus becomes incorporated within the college campus culture. Members will perceive this established group norm as the behavior with which to identify and recognize the deviance from this norm may be identifiable and entail accountability.

This particular instructional plan does provide ethical education to faculty, staff, and students. However, while the faculty and students are afforded an opportunity to actively engage in a dialog on a weekly basis, the staff may only receive ethical instruction during workshops and professional development activities.

Further recommendations concerning ethical instruction highlight several content areas that could be addressed through class discussion. Class discussion could be a viable alternative for those educators interested in a method other than the case method that is central to the proposed plan. Such topics could focus upon recent court cases, news articles, and current topics of interest. Additional discussion material could stem from general subject matter relating to computer use and the ethical implications that could result. As a final recommendation, students could be encouraged to think of future ramifications of computer use from an ethical standpoint.

Other Recommendations

Computer ethics in general must be considered an important topic to be approached regularly in virtually every area of campus life and decision-making. The importance should originate from administrative leaders then proceed on to faculty, staff, and students. Educational leaders, especially those in community colleges, should encourage participation in committees or workshops designed to improve and enforce ethics policies, procedures, and plans. Activities should be directed to instruction, research, and studies on the effectiveness of such practices. Both in demeanor and conduct, faculty, staff, and administrative personnel should promote a climate conducive to prosocial behavior and ethical conduct relating to information technology. This could consist of an outward display and verbal confirmation to others regarding obeying copyright and licensing agreements, respecting the privacy of other users, maintaining the integrity of the data contained within the system, being mindful of the proper use of resources, and refraining from downloading or viewing inappropriate materials from the Internet.

Implementation guidelines. Once a computer ethics policy is developed, administrators must give attention to implementation measures. Brown, Colter, and Short (1994) stress that the first stage of implementation should be approval by the Board of Trustees. The second stage should consist of printing the policy in the faculty and student handbooks, and the final emphasis in implementation should include making every student and computer user aware of and fully knowledgeable about the policy. The researchers suggest using registration time to introduce the policy, with additional attention provided in computer classes to reinforce the importance of its use.

Petersen and Hodges (1997) recommend making a plan for informing and communicating the computer ethics policy ahead of time. They advise utilizing student handbooks, personnel manuals, and Web-based materials. The researchers further advise that users be required to read the policy and provide some indication of understanding the concepts, such as passing a test prior to using computing resources.

Survey participants in this study contributed very little concerning implementation suggestions. If anything, this suggests that little apparently is done in this respect. One participant did propose that the computer ethics policy be addressed at the beginning of each semester within the various computer classes. This should be extended to any class prior to using the campus computing resources. Students in all programs of study should be instructed that part of the educational mission of the college is to encourage individuals to use computers ethically at all times. This includes while on campus, off campus, and after graduation.

As stated above, implementation proceedings should begin with the approval of the Board of Trustees of the college. The next group should include the Faculty Senate, college president, attorney, computer system administrator, and any additional groups or members that usually are required for policy approval and implementation procedures. At the initial meeting to discuss the policy, a committee of interested faculty, staff, and/or administrators could be appointed or assigned specifically to oversee the computer ethics policy and instructional plan.

The computer policy committee should carefully examine and make any necessary modifications or revisions to the policy and plan in a way that satisfies all those present at the initial meeting. After final approval of the materials by the committee, the following activity should be one of informing and educating others within the college concerning the computer ethics policy and plan of instruction.

The policy should first be printed within policies and procedures manuals and handbooks. This would make the materials attainable to faculty, staff, and students. Individuals could be required to read the computer ethics policy and pass a quiz prior to receiving a user code as an incentive for them to read, understand, and acknowledge the policy guidelines. Next, an abbreviated statement containing the basic precepts should be posted within each computer lab as a reminder and referral to the complete computer ethics policy.

The next phase of implementation should consist of reading and defining the policy with faculty and staff. Faculty and staff development workshops could introduce or re-introduce the policy and plan and any revisions of the policy could be addressed in subsequent workshops. The workshop might focus on the most effective methods to insure success of the computer ethics emphasis within the classroom or the laboratory. Workshop participants could receive materials designed to facilitate ethical instruction and activities by faculty or staff, as well as information relating to the most effective methods of communicating the policy to students and enforcing it. Also at this time, faculty and staff should receive their copy of the computer ethics policy and return a signed contract.

After adequate provisions are made for the faculty and staff, the next step in the implementation process can be taken. A copy of the policy and contract should be administered to the students at the beginning of each semester in each computer course as well as in other appropriate courses. Instructors should discuss the contents of the computer ethics policy and answer any questions. After a general discussion, students should sign and return the contract portion of the policy prior to logging on a computer. The computer ethics committee, system administrator, lab technician, or instructor could keep the signed contracts on file. Students could be required to sign a new contract only once during a semester, if they are taking more than one computer course. The contract will remain in effect for one year, after which, another contract will be administered with review of the policy. This process will enable any new revisions or modifications to the policy to be implemented.

While the policy discussion and contract are attended to on a once-per-semester basis, ethics instruction should continually be covered. All computer course syllabi should contain or direct students to the coverage ethics modules. The length and frequency of the modules could be determined by either the computer policy committee or left to the discretion of individual instructors. Instructors should be provided the freedom to develop the module contents as they see fit. This could range anywhere from using the entire class time for role-playing, case study, or discussion to reading a current ethics topic from a newspaper or publication.

As a final precaution in completing the implementation process, students must be required to sign in and out of open labs. This should cover other classes in which students utilize campus computing resources. Students identified at this time as not having read the policy or not having signed a contract, should be required do so.

Campus culture. For the long-term success of a computer ethics emphasis as described and outlined in this chapter, it must infiltrate the very fabric and culture of the educational institution. The effectiveness of computer ethics initiatives is dependent upon the influence of a common core of beliefs, attitudes, and customs. Faculty, staff, and students must believe that computer ethics is important and critical to the mission of the college. This is one of the reasons why the computer ethics policy should begin with the mission statement of the college.

The belief system in turn impacts the attitudes of those affected by computer ethics. The collective attitudes of faculty, staff, and students determine whether individuals decide to affirm and continue or abandon and neglect ethical issues. Finally, the belief system and attitudes ultimately influence organizational customs. Customs that facilitate ethical conduct will emerge in a culture that believes in computer ethics in general and ethical behavior in all dimensions of college life. This will help insure long-term success by maintaining accountability between existing members and enabling new members to adapt positive norms of behavior.

Contributions of the study. The findings from this study contribute to the existing body of literature and scholarly research on computer ethics issues, policies, and educational instruction. This contribution to research may assist other scholars in their endeavor to help determine what educational leaders think about current problems and issues as well as viable solutions. In addition, the findings of this study may contribute to scholars' understanding of computer technology ethics within current educational settings and should raise new questions about computer ethics that scholars can pursue.

Evidence provided by this study emphasizes the need for and benefits of creating and implementing a computer ethics policy. A model policy and ethical instruction, based on a more comprehensive understanding of the ethical issues and problems and rooted in significant behavioral assumptions, could be a practical solution for those educational leaders searching for one.

The findings from this study clarify, identify, and confirm the practical problems and concerns facing educational leaders due to the prominence and use of information technology on college campuses. While a special emphasis of this study was computer ethics issues, needs, and solutions within the community college setting and particularly within the North Carolina Community College System, this information may also apply to other institutions of higher education and other regions. This information may be useful in guiding other educators and researchers interested in the ongoing study of computer ethics issues and concerns. It should be particularly valuable to those interested in closer scrutiny of the underlying principles and theoretical concepts that promote and facilitate ethical conduct by computer users.

A second major contribution is a model computer ethics policy and ethical instruction plan for educators interested in viable solutions to the ethical dilemmas they face. The perfecting of the policy and plan began with a careful analysis of successful computer ethics policies of other educational institutions. This resulted in a draft proposal for a model computer ethics policy and implementation plan for ethical instruction. Participants in the study provided thoughtful consideration and feedback after examining of the policy and plan that contributed to a revised computer ethics policy and instructional plan. While the policy and plan are particularly applicable to the North Carolina Community College System, many of its components are pertinent to other institutions of higher education as well.

The final contribution of this research is that it elicits support for the utilization of the Theory of Deindividuation. As discussed earlier, this theory is one of the few behavioral theories identified by scholars as useful in understanding motivational forces and computer user behavior. In addition, this theory considers both a personal and social identity necessary in the assumptions of driving forces that impact human behavior. The findings from this study may provide scholars with new insights regarding the theory and its practical applications, and demonstrate to educational leaders the value of the theory as framework through which to explore computer ethics issues.

In addition, the findings clearly show that the theory is helpful in exploring and determining the underlying assumptions of computer users. Thus, this study helps validate the basic concepts that comprise the theory and its utility for assisting educators and others interested in developing and implementing computer ethics policies and procedures that will promote and facilitate ethical behavior.

Directions for future research. This study clearly reveals that there is a need for more scholarly research dealing with computer ethics, computer policies, and computer instruction in the educational setting. To better equip educational leaders for addressing technology-induced ethical concerns, further research is necessary using a variety of research methodologies. Research is needed within the area of computer ethics instruction and more specifically computer ethics policies and their effectiveness.

The scope of this study was limited to the North Carolina Community College System. While the results of this study are certainly applicable to community colleges and other educational institutions within North Carolina and nationally, more research is needed. As the future of education becomes more technology-driven and technology-dependent, further studies are necessary for analyzing and anticipating the impact and implications of such a trend.

Scholarly research and empirical evidence on computer ethics behavior and the effectiveness of various computer ethics policies and instruction are needed to enrich and add to the existing body of research. Other educational and organizational institutions or settings should be examined to gain a more thorough understanding of computer ethical issues. Better demographic and psychographic profiles of computer users in educational environments need to be developed. Studies should not be limited to just students, but rather all users of computing resources.

Future studies could be conducted with a larger sampling size. A greater number of participants would enable a more thorough examination, utilizing factor analysis, multiple regression and other commonly used statistical analyses.

Research is also needed to determine empirically if computer ethics policies do make a significant difference on behavior. Studies that use pretest/posttest designs could yield particularly meaningful data.

Studies are needed to test the Theory of Deindividuation further as a valid framework to predict behavior and facilitate ethical conduct. Research could be conducted that examines how individuals identify with others through the computer as opposed to identifying with others face-to-face. Studies could be undertaken to determine if being physically present with a group in a room and communicating with them through the computer made a difference in behavior. In addition, research could be conducted to determine if embedding elements based on the theory into computer ethics policies, such as student contracts, do impact user behavior.

Finally, more qualitative analyses are needed to determine at a more personal level how best to educate individuals in ethical and prosocial computing behavior. Qualitative studies could include both observed behavior of computer users and in-depth interviews of system administrators and computer users. Combining a quantitative approach and qualitative approach to this issue will assist greatly in the development of information that is valid and useful to educators and administrators.

Summary

As discussed previously, organizational leaders within higher education have a unique opportunity to help educate computer users to make prosocial choices when faced with ethical dilemmas. The literature supports the use of computer ethics instruction and computer ethics policies as effective measures in facilitating ethical conduct by computer users. In addition, the body of research regarding the study of behavioral models, particularly the Theory of Deindividuation, indicates that an increased understanding and awareness of the underlying factors involved in unethical behavior are possible through the application of such theories.

Based upon the information acquired through the survey of community college administrators, and what was found in previous research and supporting literature, the model computer ethics policy presented in Appendix M should basically serve the needs of students, faculty, and staff within the North Carolina Community College System. This proposed computer ethics policy should not only assist North Carolina Community College System administrators but could aid other educational leaders plagued by information technology concerns and issues.

Equipped with the knowledge that information technologies have become a necessity, one may safely conclude that ethical issues involving computers will continue to be a topic of discussion among organizational leaders. One may also assume that given the increasing demand for improvements and resulting rapidly changing nature of technologies, new ethical dilemmas are certain to occur. Scholars must be encouraged and guided in developing more effective measures, policies, and instruction to insure that computer ethics remains a current and informative area. Leaders in higher education in search of effective solutions to computer-related ethical dilemmas must anticipate that ethical issues will continue and evolve. They must draw from and participate in scholarly research on this subject and apply it to computer ethics needs on their campuses. The ethical climate at not only their particular colleges, but also the future of ethical behavior in a computer dependent society may be at stake.

References

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuh. & J. Beckmann (Eds.), Action-control: From cognition to behavior (pp. 11-39). Heidelberg: Springer.

Ajzen, I. (1988). Attitudes, personality, and behavior. Chicago: Dorsey Press.

Ajzen, I., & Fishbein, M. (1972). Attitudes and normative beliefs as factors influencing behavioral intentions. Journal of Personality and Social Psychology, 21, 1-9.

Alexander, M. (1989, April). Strong scruples can curb computer crime. Computerworld, 23, p. 100

Alfred, R. L. (1980). Socioeconomic impact of two-year colleges. (Report No. JC 800 124). (ERIC Document Reproduction Service ED 181 983)

Anderson, J. A. (1996, June). Ethics, privacy, and security in higher education technology. Paper presented at the meeting of the Association of Small Computer Users in Education, North Myrtle Beach, SC.

Arlow, P., & Ulrich, T. A. (1983, Spring). Can ethics be taught to business students? The Collegiate Forum, p. 17.

Arnold, V. (1995). Ethics instruction for workforce development. Unpublished paper, East Carolina University, at Greenville, NC.

Barger, R. (1998). University of Notre Dame: Electronic Information Processing: Studying Computer Ethics, The Internet, & The Web Syllabus [On-line]. Available: http://www.nd.edu/~rbarger/capp471syl.html.

Baron, P., & Others. (1984). Business students' perceptions of corporate ethical behavior. (Report No. HE 017 580). (ERIC Document Reproduction Service ED 247

861)

Baumhart, R. S. (1968). An honest profile: What businessmen say about ethics in business. New York: Holt, Rinehart and Winston.

Beck, L. G., & Murphy, J. (1993, October). Preparing ethical leaders: Overviewing current efforts and analyzing forces that have shaped them. Paper presented at the meeting of the University Council for Educational Administration, Houston, TX.

Beck, L., & Ajzen, I. (1991). Predicting dishonest actions using the theory of planned behavior. Journal of Research in Personality, 25, 285-301.

Benkelman, S. (1995, December 30). Ban on Internet is decried, defied. Newsday [On-line].

Betts, M. (1994, June). Campaign addresses computer ethics void. Computerworld, 28, p. 21.

Betts, M. (1995, May). Dirty Rotten Scoundrels? Computerworld [On-line].

Bickel, R. W., Larrondo-Petrie, M. M., & Bush, D. F. (1992). EDICT for computer ethics education. Journal of Systems Software, 17, 81-89.

Brown, L., Colter, L. W., & Short, T. (1994, June). Developing a campus-wide computer ethics policy. Paper presented at the meeting of Association of Small Computer Users in Education, North Myrtle Beach, SC.

Budden, S. C. (1984). Communications and information technologies in community colleges in Canada. (Report No. IR 014 617). Toronto, Ontario: Office of Development Research. (ERIC Document Reproduction Service No. ED 323 972)

Bunn, D. N., Caudill, S. B., & Gropper, D. M. (1992). Crime in the classroom: An economic analysis of undergraduate student cheating behavior. Journal of Economic

Education, 23, 197-207.

Burnett, K. L. (1996). Ethics and IT: Is the human factors approach an ethical way of designing and implementing information technology? In J. Kizza (Ed.), Social and ethical effects of the computer revolution. (pp. 98-123). Jefferson, NC: McFarland and Company, Inc.

Callahan, D., & Bok, S. (1979). The role of applied ethics in learning. Change, 11, 23-27.

Cannavale, F. J., Scarr, H. A., & Pepitone, A. (1970). Deindividuation in the small group: Further evidence. Journal of Personality and Social Psychology, 16, 141-147.

Cetron, M. (1988). Seventy-one trends that may affect entrepreneur education for future world markets. Paper presented at the National Entrepreneurship Education Forum, Boston, MA.

Chaney, L. H., & Simon, J. C. (1994). Strategies for teaching computer ethics. The Journal of Computer Information Systems, 35, 1.

Cobb, N. (1996, April 16). "Schools take on info-highway patrol." The Boston Globe, p. 27.

Cohen, A. M., & Brawer, F. B. (1996). The American Community College. (3rd Ed.). Jossey-Bass Publishers: San Francisco.

Cole, B. C., & Smith, D. L. (1995). Effects of ethics instruction on the ethical perceptions of college business students. Journal of Education for Business, 70, 351-356.

Connolly, F. W. (1995). Intellectual honesty in the era of computing. T.H.E. Journal, 22, 86-88.

Connolly, M. V. (1997, June). Ethical issues involving the Internet. Paper presented at the meeting of the Association of Small Computer Users in Education, North Myrtle Beach, SC.

Cooley, W. W. (1990). Confidentiality of education data and data access. (Tech. Rep. No. 7). Pennsylvania: Pittsburgh University, PA Learning Research and Development Center.

Couger, J. D. (1989). Preparing IS students to deal with ethical issues. MIS Quarterly, 13, 211-216.

Day, B. C., & Day, P. C. (1996). The Internet and ethics: Dilemma and decisions for institutions of higher education. In J. Kizza (Ed.), Social and ethical effects of the computer revolution. (pp. 53-60). Jefferson, NC: McFarland and Company, Inc.

Day, K., & Schrum, L. (1995). The Internet and acceptable use policies: What schools need to know. The ERIC Review, 4, 9-11.

DeGeorge, R. T. (1990). Business Ethics (2nd ed.). Macmillan: New York.

Dejoie, R., Fowler, G., & Paradice, D. (Eds.). (1991). Ethical issues in information systems. Boston: Boyd & Fraser Publishing Company.

DeLoughry, T. J. (1988, February). Failure of colleges to teach computer ethics is called oversight with potentially catastrophic consequences. The Chronicle of Higher Education, A15-A16.

DeLoughry, T. J. (1993, January). Colleges try to devise policies on obscenity on campus networks. The Chronicle of Higher Education, A27-A28.

DeLoughry, T. J. (1995, May). Well-appointed web pages. The Chronicle of Higher Education, A19-A21.

DeMaio, H. B. (1991). Information ethics—it does not come naturally. Computer Security Journal, 5, 1.

DeMaio, H. B. (1990, April). Information ethics, a private perspective. Paper presented at the meeting of the National Institute of Justice Professional Conference on Information Technology Ethics, Washington, DC.

Demmon, T., & Others. (1996). Moral and character development in public education (Report No. SO 027 606). (ERIC Document Reproduction Service No. ED 409 251)

Denning, D. E., & Lin, H. S. (1994). Rights and responsibilities of participants in networked communities. (Report No. ISBN 0-309-0-5090-1, pp. 17-84). Washington, DC: National Academy of Sciences.

Diener, E. (1979). Deindividuation, self-awareness, and disinhibition. Journal of Personality and Social Psychology, 37, 1160-1171.

Diener, E. (1980). Deindividuation: The absence of self-awareness and self-regulation in group members In P. Paulus (Ed.), The psychology of group influence. Hillsdale, NJ: Erlbaum.

Diener, E., Lusk, R., DeFour, D., & Flax, R. (1980). Deindividuation: Effects of group size, density, number of observers, and group member similarity on self-consciousness and disinhibited behavior. Journal of Personality and Social Psychology, 39, 449-459.

Dodd, D. K. (1985). Robbers in the classroom: A deindividuation exercise. Teaching of Psychology, 12, 89-91.

DuFrene, D., & Others. (1990). Investigation of a technique for measuring ethical development of students in business: A heuristic example. Paper presented at the meeting of the Mid-South Educational Research Association, New Orleans, LA.

Eaton, J. S. (1994). Strengthening collegiate education in community colleges. San Francisco, CA: Jossey-Bass Inc.

Emswiller, R., Deaux, K., & Willits, J. (1971). Similarity, sex and requests for small favors. Journal of Applied Social Psychology, 1, 284-291.

Ethics and the Internet create dilemmas for public schools. (1997, September 11). Business Wire [On-line].

Ethics—Business Educators Teach Students to do the right thing! (1997, January). Keying In. 1-8.

Exon, J. (1996, February). Internet privacy: How far should federal regulation go? Computerworld. [On-line].

Festinger, L., Pepitone, A., & Newcomb, T. (1952). Some consequences of deindividuation in a group. Journal of Abnormal Social Psychology, 47, 382-389.

Fishbein, M. (1963). An investigation of the relationships between beliefs about an object and the attitude toward that object. Human Relations, 16, 233-240.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: An introduction to theory and research. Addison-Wesley: Reading, MA.

Fisher, C. S. (1975). The affects of urban life on traditional values. Social Forces, 53, 420-432.

Fodor, J. L. (1996). Human values in the computer revolution. In J. Kizza (Ed.), Social and ethical effects of the computer revolution. (pp. 256-266). Jefferson, NC: McFarland and Company, Inc.

Friedman, B. (1990, April). Moral responsibility and computer technology. Paper presented at the meeting of the American Educational Research Association, Boston, MA.

Friedman, B. (1990, April). Societal issues and school practices: An ethnographic investigation of the social context of school computer use. Paper presented at the meeting of the American Educational Research Association, Boston, MA.

Fritz, J. (1995, June 12). Untangling your way onto the Web. Network World, p. 56.

Gilliland, K., & Pollard, M. (1984). Ethics and computer use. Mathematics Teacher, 77, 598-603.

Gotterbarn, D. (1992). The use and abuse of computer ethics. Journal of Systems Software, 17, 75-80.

Gotterbarn, D. (1998). Computer ethics: Responsibility regained. Unpublished manuscript, East Tennessee University at Johnson City.

Grabow, P. C. (1996). La technique: An area of discourse for computers in society. In J. Kizza (Ed.), Social and ethical effects of the computer revolution. (pp. 298-312). Jefferson, NC: McFarland and Company, Inc.

Green, K. C. (1996). Campus computing, 1996. The seventh national survey of desktop computing and information technology in American higher education. (ERIC Document Reproduction Service No. ED 405 762)

Greenberg, D. S. (1986, November 4). Computers put the byte on privacy. Washington Post [On-line].

Gregory, E. (1994, June 28). Keeping computer porn out of the classroom.

Gannett News Service [On-line].

Hegarty, W. H., & Sims, H. P. (1978). Some determinants of unethical decision behavior. Journal of Applied Psychology, 63, 451-457.

Hegarty, W. H., & Sims, H. P. (1979). Organizational philosophy, policy, and objectives related to unethical decision behavior: A laboratory experiment. Journal of Applied Psychology, 64, 331-338.

Hersh, R. H., & Pagliuso, S. (1977). A comparison of two moral education surveys: US and Ontario educators. Phi Delta Kappan, 58, 773-74.

Hiltz, S. R., Turoff, M., & Johnson, K. (1989). Experiments in group decision making: Disinhibition, deindividuation, and group process in pen name and real name computer conferences. Decision Support Systems, 5, 217-232.

Hoffman, L. J., & Clark, P. C. (1991, February). Imminent policy considerations in the design and management of national and international computer networks. IEEE Communications, 29, 68-74.

Hunt, N. P., & Paplewis, R. (1989, November). Educational computing: Ethical issues for school administrators and policy makers. Paper presented at the meeting of the California Educational Research Association, San Francisco, CA.

Internet indecency: National Education Association. National Education Association Statement of the National Education Association Submitted to the Committee on Commerce, Science, and Transportation US Senate on Indecency on the Internet. (1998, February 10). (Congressional Testimony). Federal Document Clearing House, Inc.

Johnson, D. G. (1985). Computer ethics. Prentice Hall, Englewood Cliffs, NJ.

Johnson, D. G. (1991, summer). Computers and ethics. Phi Kappa Phi Journal, 15-17.

Johnson, D. G. (1994). Computer Ethics (2^{nd} ed.). Upper Saddle River, NJ: Prentice Hall.

Johnson, D. G., & Snapper, J. W. (1985). Ethical issues in the use of computers. Belmont, CA: Wadsworth Publishing Company.

Jones, D. (1998, April 27). Balancing ethics and technology: Companies grapple with limiting employee abuse. USA Today [On-line].

Josephson, J., & Josephson, E. (1992). The hole in the moral ozone: Ethical values, attitudes, and behaviors in American schools. (Available from the Joseph and Edna Josephson Institute of Ethics)

Kallman, E. A. (1992). Developing a code for ethical computer use. Journal of Systems Software, 17, 69-74.

Kamay, V., & Adams, T. (1992). The 1992 profile of computer abuse in Australia. The Australian Computer Abuse Research Bureau at the Royal Melbourne Institute of Technology, Australia.

Kiesler, S. (1986, January/February). The hidden messages in computer networks. Harvard Business Review, 46-58.

Kiesler, S., Siegel, J., & McGuire, T. W. (1984). Social psychological aspects of computer-mediated communication. American Psychologist, 39, 1123-1134.

Kizza, J. M. (1996). Social and ethical effects of the computer revolution. Jefferson, NC: McFarland and Company, Inc.

Kohlberg, L. & Kandee, E. (1981). Relationship of moral judgment and moral action. Paper presented at the Florida International University Conference.

Larrabee, J. (1994, September 26). Cyberspace a new beat for police. USA Today, p. 01.

Latimore, R. R. (1997). The electronic library and the on-line classroom: A technical, legal, ethical, and moral perspective. (Report No. IRO 056 713). (ERIC Document Reproduction Service No. ED 412 981)

Laudon, K. C. (1995). Ethical concepts and information technology. Communications of the ACM, 38, 33-39.

Lea, M., & Spears, R. (1991). Computer-mediated communication, de-individuation and group decision-making. International Journal of Man-Machine Studies, 34, 283-301.

LeBon, G. (1896). The crowd. London: Ernest Benn.

Leventhal, L. M., Instone, K. E., & Chilson, D. W. (1992). Another view of computer science ethics: Patterns of responses among computer scientists. Journal of Systems Software, 17, 49-60.

Lewis, C. W. (1993, Summer). Ethics and information technology: Operating in virtuous reality. The Public Manager: The New Bureaucrat, 46-50.

Loch, K. D., & Conger, S. (1996). Evaluating ethical decision making and computer use. Communications of the ACM, 39, 74-83.

Magner, D. K. (1989). Students urge graduate business schools to emphasize ethical behavior and require courses in standards. The Chronicle of Higher Education, 35, A31-32.

Marker, G. (1996, November). Social studies and the Internet: Developing a school policy. Unpublished manuscript.

Mason, R. (1986). Four ethical issues of the information age. MIS Quarterly, 10, 5-12.

Matheson, K., & Zanna, M. P. (1988). The impact of computer-mediated communication on self-awareness. Computers in Human Behavior, 4, 221-233.

McAllester, M. (1998, September 30). Identity crisis: Theft of personal information, commercial abuses and terrorist threats fuel debate over the future of the Net. Newsday, p. C03. [On-line].

McCain-Hollings introduce Internet School Filtering Act. (1998, February 9). (Capitol Hill Press Release). Federal Document Clearing House, Inc.

Milgram, S. (1965). Some conditions of obedience and disobedience to authority. Human Relations, 18, 57-76.

Miller, G. (1998, October 1). Web copyright suit goes to heart of debate: LA Times, Washington Post take action against free republic which copies and posts their articles. Los Angeles Times [On-line].

Miller, P. F., & Coady, W. T. (1984). Vocational ethics: Toward the development of an enabling work ethic. Springfield: Illinois State Board of Education.

Moor, J. H. (1985) What is computer ethics? Metaphilosophy, 16, 266-275.

Morris, A. B. (1996). Effective information management: A question of ethics? In J. Kizza (Ed.), Social and ethical effects of the computer revolution. (pp. 32-44). Jefferson, NC: McFarland and Company, Inc.

Murphy, P. R., & Boatright, J. R. (1994). Assessing the effectiveness of instruction in business ethics: A longitudinal analysis. Journal of Education for

Business, 69, 326-32.

Neumann, P. G. (1991). Computers, ethics, and values: Inside risks. Communications of the ACM, 34, 106.

North Carolina Community College System fact book. (1999). Raleigh, NC: North Carolina Community College System [On-line]. Available: http://www.ncccs.cc.nc.us

O'Brien, W. A. (1989). A liberal education for business ethics. (Report No. SO 030 179). (ERIC Document Reproduction Service ED 323 143)

Ownby, A. C., & Moses, D. R. (1994, Spring). A comparison of computing ethics perceptions of information systems students and other business administrator students. Office Systems Research Journal, 12, 33-43.

Oz, E. (1992, December). Ethical standards for information systems professionals: A case for a unified code. MIS Quarterly: Management Information Systems, 423-433.

Oz, E. (1994). Ethics for the information age. Business and Educational Technologies, 76.

Palinchak, R. (1973). The evolution of the community college. Metuchen, NJ: The Scarecrow Press, Inc.

Palmiter, C. W. (1996). A call for responsibility for ethical behavior in information technology. In J. Kizza (Ed.), Social and ethical effects of the computer revolution. (pp. 230-247). Jefferson, NC: McFarland and Company, Inc.

Parker, D. (1976). Crime by computer. Charles Scribner's Sons.

Parker, D. (1978). Ethical conflicts in computer science and technology. Menlo

Park, CA: SRI International.

Parker, D. R., Swope, S., & Baker, B. N. (1990). Self-assessment: Procedure XXII. Communications of the ACM, 33, 110-132.

Pavela, G. (1996, Spring). Esteven J. McDonald on: Electronic communications and the law on campus [On-line]. Available: http://www.cornell.edu

Petersen, R. J., & Hodges, M. W. (1997). Legal, ethical, and policy issues. New Directions for Student Services, 78, 45-58.

Petrick, J. A. (1992). Organizational ethics development: Implications for human resource professionals. Journal of Education for Business, 67, 330-334.

Pietrucha, B. (1998, February 10). Bill would filter Internet access to schools. Newsbytes News Network [On-line].

Pietrucha, B. (1998, February 27). Federal Judge Rejects Virginia Internet Decency Law. Newsbytes News Network [On-line].

Pollack, T. A. (1994, June). Ethical issues for information systems professionals. Paper presented at the meeting of the Association of Small Computer Users in Education, North Myrtle Beach, SC.

Pratt, C. B., & McLaughlin, G. W. (1989). An analysis of predictors of college students' ethical inclination. Research in Higher Education, 30, 195-219.

Pulliam, S. C. (1994). Ethics and computer scientists: In recreating the revolution. Paper presented at the meeting of the National Educational Computing Conference, Boston, MA.

Ravitz, J. (1995). Ethics in scholarly communications: Intellectual property and new technologies. (ERIC Document Reproduction Service Ed 409 864)

Reicher, S. D. (1984). Social influence in the crowd: Attitudinal and behavioral effects of de-individuation in conditions of high and low group salience. The British Journal of Social Psychology, 23, 341-350.

Riser, R. & Gotterbarn, D. (1996). Ethics activities in computer science courses. Computers and Society, 26, 13.

Robinson, W. (1999). Duke University: Ethics and the Internet Syllabus [On-line]. Available: http://www.duke.edu/~wgrobin/ethics/.

Roderick, J. C., Jelley, H. M., Cook, J. R., & Forcht, K. A. (1991). The issue of white collar crime for collegiate schools of business. Journal of Education for Business, 66, 287-290.

Rubin, R. (1996). Moral distancing and the use of information technologies: The seven temptations. In J. Kizza (Ed.), Social and ethical effects of the computer revolution. (pp. 124-135). Jefferson, NC: McFarland and Company, Inc.

Sadalla, E. K. (1978). Population size, structural differentiation, and human behavior. Environment and Behavior, 10, 271-291.

Saunders, L. (1994 May 22). Ethics in Cyberspace. Unpublished paper, University of Nevada, at Las Vegas.

Sheel, S. J., & Collins, E. E. (1997, June). Evaluating the effectiveness of a formal ethics component in the computer science curriculum. Paper presented at the meeting of the Association of Small Computer Users in Education, North Myrtle Beach, SC.

Siegel, J., Dubrovsky, V., Kiesler, S. & McGuire, T. W. (1986). Group processes in computer-mediated communication. Organizational Behavior and Human Decision

Processes, 37, 157-187.

Singer, J. E., Brush, C. A., & Lublin, S. C. (1965). Some aspects of deindividuation: Identification and conformity. Journal of Experiments in Social Psychology, 1, 356-378.

Sivin, J. P., & Bialo, E. R. (1992). Ethical use of information technologies in education: Important issues for America's schools. Washington, DC: US Department of Justice, Office of Educational Research and Improvement.

Slater, D. (1991, October 14). New crop of IS pros on shaking ground. Computerworld, p. 90.

Slater, D. (1994, December 5). Cyberspace and the law. Computerworld, p. 114.

Sowell, T. (1997, December 17). Burden pornographers, not parents. Rocky Mountain News [On-line].

Spears, R., Lea, M., & Lee, S. (1990). De-individuation and group polarization in computer-mediated communication. The British Journal of Social Psychology, 29, 121-134.

Sproull, L., & Kiesler, S. (1986). Reducing social context cues: Electronic mail in organizational communication. Management Science, 32, 1492-1512.

Stewart, K., & Felicetti, L. (1996). The attitudes of business majors in Australia and the United States toward the teaching of business ethics. Journal of Education for Business, 71, 363-367.

Sullivan, P. (1996). Ethics in the computer age. In J. Kizza (Ed.), Social and ethical effects of the computer revolution. (pp. 288-295). Jefferson, NC: McFarland and Company, Inc.

Summers, C., & Markusen, E. (1992). Computers, ethics, and collective violence. Journal of Systems Software, 17, 91-103.

Survey reveals America's longing for ethics and personal responsibility. (1997, September 19). Business Wire [On-line].

Trebilcock, B. (1997, April). Child molesters on the Internet: Are they in your home? Redbook, 188, 100.

Turner, J. C. (1982). Towards a cognitive redefinition of the social group. In H. Taifel (Ed.). Social identity and intergroup relations. Cambridge: Cambridge University Press.

Tweet, M. (1998, February 19). Taxpayers support pornography in local libraries. The Columbian [On-line].

US Congress, Office of Technology Assessment (1986). Intellectual property rights in an age of electronics and information. (DHHS Publication No. OTA-CIT-302). Washington, DC: US Government Printing Office.

US Department of Commerce, Bureau of the Census. (1997). Current Population Survey. Unpublished data.

US Department of Education, National Center for Education. (1998). Statistics, fast response survey system, advanced telecommunications in us elementary and secondary public schools, fall 1996, and Internet access in public schools and classrooms: 1994-98. Unpublished data.

US Senator Dan Coats holds news conference with others to discuss access to Internet sites. (1997, December 1). Washington Transcript Service [On-line].

Vieira, M. (1998, February 27). Web regulation still far off, professors say.

Independent Florida Alligator [On-line].

Vitell, S. J., & Davis, D. L. (1990). Ethical beliefs of MIS professionals: The frequency and opportunity for unethical behavior. Journal of Business Ethics, 9, 63-70.

Walden, R., & Gordon, D. (1988). Survey indicates ethics have place in curriculum. Unpublished paper.

Ward, S. P., Ward, D. R., & Wilson, T. E. (1996). The code of professional conduct: Instructional impact on accounting students' ethical perceptions and attitudes. Journal of Education for Business, 71, 147-150.

Weizenbaum, J. (1969). The two cultures of the computer age. Technology Review, 71, 54-57.

Weston, R. (1996, September 9). The Internet: Managing the connection. Computerworld.

Wilder, D. A. (1978). Reduction of intergroup discrimination through individuation of the out-group. Journal of Personality and Social Psychology, 36, 1361-1374.

Wilson, D. T., Mathews, H. T., & Harvey, J. W. (1975). An empirical test of the Fishbein Behavioral Intention Model. Journal of Consumer Research, 1, 39-48.

Winn, K. (1996). Policies to manage control of content on college and university web sites. Unpublished manuscript, Syracuse University at NewYork.

Worchel, S., & Andreoli, V. A. (1977). Intergroup cooperation and intergroup attraction: The effect of previous interaction and outcome of combined effort. Journal of Experimental Social Psychology, 13, 131-140.

Zemke, R. (1977). Ethics training: Can we really teach people right from wrong? Training HRD, 14, 37-41.

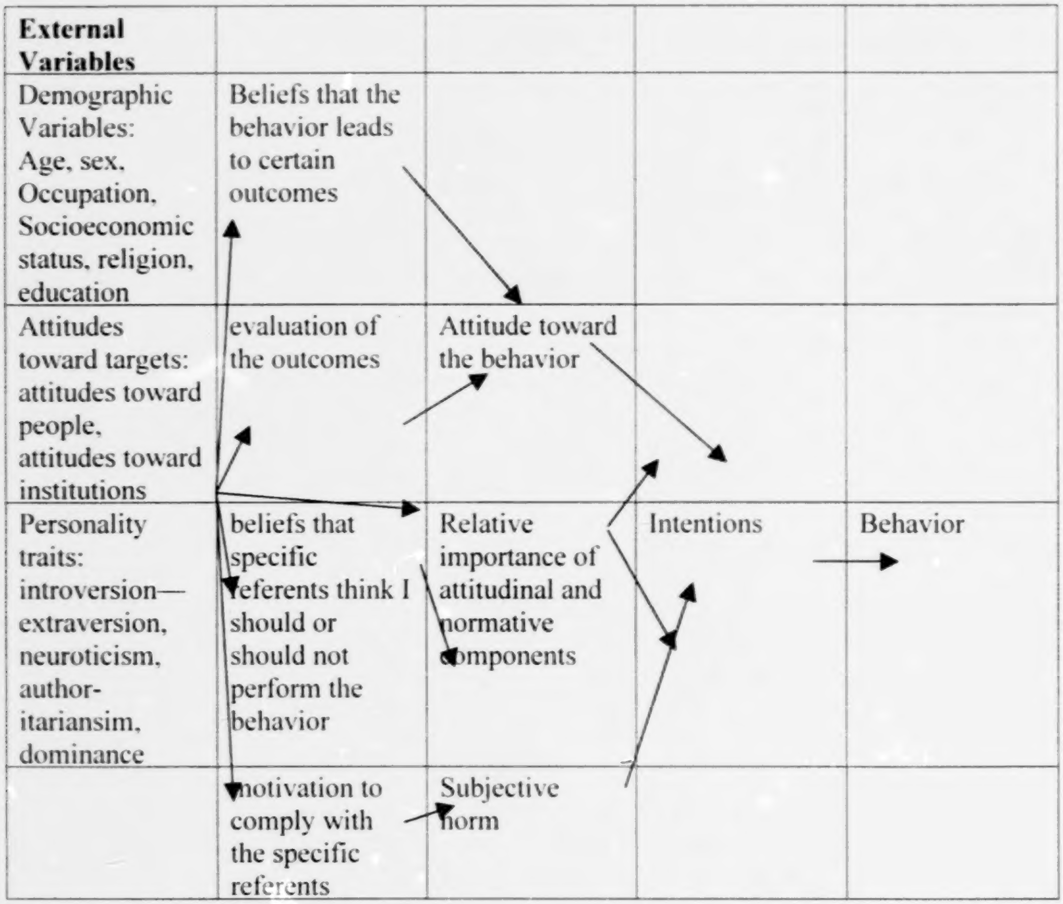
Ziller, R. C. (1964). Individuation and socialization. Human Relations, 17, 341-360.

Zimbardo, P. G. (1969). The cognitive control of motivation. Glenview, IL: Scott Foresman.

Zimbardo, P. G. (1970). The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos. In W. J. Arnold & D. Levine (Eds.), Nebraska Symposium on Motivation: Vol. 17. Lincoln: University of Nebraska Press.

Appendix A:
Fishbein's Behavioral Intention Model

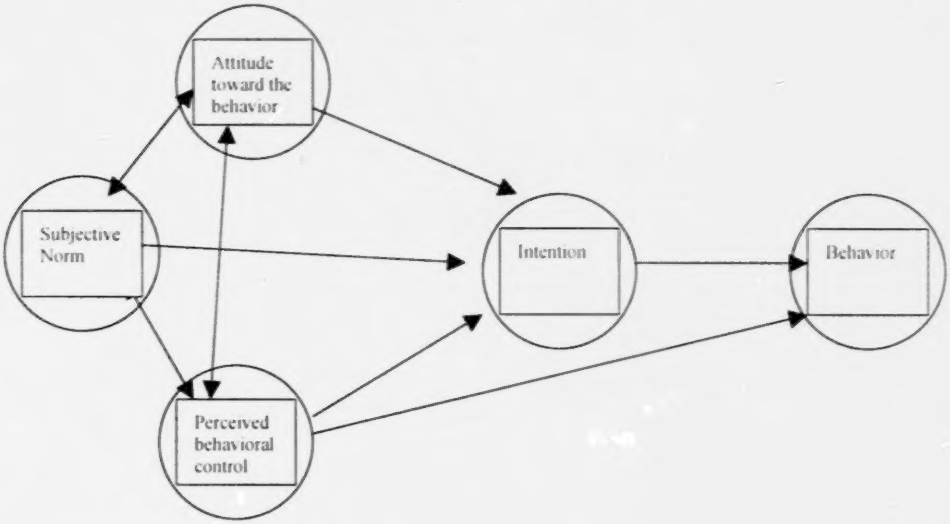
Figure 1. Fishbein and Ajzen's Model of Reasoned Action: Influence of external variables on beliefs, attitudes, intentions, and resulting behavior.



External Variables				
Demographic Variables: Age, sex, Occupation, Socioeconomic status, religion, education	Beliefs that the behavior leads to certain outcomes			
Attitudes toward targets: attitudes toward people, attitudes toward institutions	evaluation of the outcomes	Attitude toward the behavior		
Personality traits: introversion—extraversion, neuroticism, authoritariansim, dominance	beliefs that specific referents think I should or should not perform the behavior	Relative importance of attitudinal and normative components	Intentions	Behavior
	motivation to comply with the specific referents	Subjective norm		

Appendix B:
Theory of Planned Behavior

Figure 2. Theory of Planned Behavior: Influence of subjective norm on attitude, perception, intention, and resulting behavior.


Attitude toward the behavior
Subjective Norm
Intention
Behavior
Perceived behavioral control

Appendix C:
Theory of Deindividuation

Figure 3. Theory of Deindividuation: Representation of the Deindividuation Process. Demonstrates how input variables cause minimization of inferred subjective changes with resulting output behaviors.

Input Variables	**Inferred Subjective Changes**	**Output Behaviors**
A. Anonymity	**Minimization of:**	a. Behavior emitted is emotional, impulsive, irrational, regressive, with high intensity
B. Responsibility: shared, diffused, given up	1. Self-observation-evaluation	b. Not under the controlling influence of usual external discriminative stimuli
C. Group size, activity	2. Concern for social evaluation	c. Behavior is self-reinforcing and is intensified, amplified with repeated expressions of it
D. Altered temporal perspective: present expanded, future and past distanced	↓	d. Difficult to terminate
E. Arousal	Weakening of controls based upon guilt, shame, fear, and commitment	e. Possible memory impairments; some amnesia for act.
F. Sensory input overload	↓	f. Perceptual distortion—insensitive to incidental stimuli and to relating actions to other actors
G. Physical involvement in the act	Lowered threshold for expressing inhibited behaviors.	g. Hyper-responsiveness "contagious plasticity" to behavior of proximal, active others

Appendix D:
North Carolina Integrated Information Network Policy

USE OF THE NORTH CAROLINA INTEGRATED INFORMATION NETWORK AND THE INTERNET

Purpose

To establish a policy pertaining to the use of the North Carolina Integrated Information Network (NCIIN) and the global Internet by public staffs

Background

The Internet is a world-wide collection of interconnected networks. The State's wide area network, the NCIIN, is one of many networks connected to the Internet. Electronic tools associated with Internet access, such as electronic mail (E-mail) and the World Wide Web(), help public agencies streamline information access and conduct business. These tools are used with the NCIIN to facilitate inter-agency communication and information processing. These same tools are used for communications between public agencies and entities on the Internet, such as other government organizations, educational institutions, private businesses, and citizens.

There are many parallels between the new electronic information tools and older technologies used for similar purposes (for example, telephones and written correspondence). As such, the same general concepts of professionalism and appropriate use of publicly owned or publicly provided information processing resources apply.

Increasing numbers of public staffs now access the Internet. Public use of publicly provided information on the NCIIN is also growing. Public staffs have stewardship responsibilities for public information. The open connection afforded by Internet access underscores the need for heightened awareness among public employees regarding prudent behavior as it pertains to information dissemination and access.

The Information Resource Management Commission adopted a "Policy and Guidelines on the Use of the Internet" on August 2, 1994. That Policy and Guidelines remains the governing guidance to appropriate use of the NCIIN and the Internet by public staffs. The following policy represents the mandated application of certain aspects of that Policy and Guidelines.

Scope

This policy applies to all government agencies under the authority of the Information Resource Management Commission (IRMC).

Policy

1. While in performance of work-related functions, while on the job, or while using publicly owned or publicly provided information processing resources, public employees are expected to use the NCIIN and the Internet responsibly and professionally and shall make no intentional use of these services in an illegal, malicious, or obscene manner. Public employees may make reasonable personal use of publicly owned or provided NCIIN or Internet resources as long as:

a. The direct measurable cost to the public is none or is negligible;

b. There is no negative impact on employee performance of public duties;

c. The policy is applied equitably among all employees of the agency;

d. Employees shall reimburse the agency if costs are incurred, provided that costs may be incurred only in critical situations.

2. When sending or forwarding E-mail over the NCIIN or the Internet, public employees shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden.

3. Public employees have a responsibility to make sure that all public information disseminated via the NCIIN and the Internet is accurate. Employees shall provide in association with such information its source and the date at which it was current and an electronic mail address allowing the recipient to contact the public staffs responsible for making the information available in its current form.

4. All files downloaded from a source external to the NCIIN must be scanned for viruses. This includes files obtained as e-mail attachments and by any other file transfer mechanism. It is the responsibility of public employees to prevent the introduction or propagation of viruses.

5. The Internet provides easy access to software distributed by companies on a trial basis. This free access does not indicate that the software is free or that it may be distributed freely. All applicable software copyright and licensing laws must be followed.

Definitions

E-Mail: Electronic Mail - The capability to compose, address, and send messages electronically.

NCIIN: North Carolina Integrated Information Network - refers to a web of interoperable networks, within the state, that transmits data, text, images, voice, and video.

: World Wide Web - The integrated world wide network of computers based on the hypertext transfer protocol (HTTP), and Transmission Control Protocol/Internet Protocol (TCP/IP), commonly used to bring information to computer users via a client browser program.

Information processing resources: Electronic computing and communications hardware, software, networks, and information.

Recommended Review Frequency

The recommended review frequency for this policy is every six months.

Last Review Next Review Reviewer Change Recommended?

Additional References

State of North Carolina, Information Resource Management Commission, "Policy and Guidelines on the Use of the Internet," adopted August 2, 1994, http://www.sips.state.nc.us/IRMC/documents/approvals/irmcinet.html

Approved by the IRMC September 1996

Appendix E:
North Carolina Community Colleges

ALAMANCE COMMUNITY COLLEGE
Graham, NC
Director/Network Administrator: Dennis Rasmussen

ASHEVILLE-BUNCOMBE TECHNICAL COMMUNITY COLLEGE
Asheville, NC
Primary System Administrator: David McKinney

BEAUFORT COUNTY COMMUNITY COLLEGE
Washington, NC
Primary System Administrator: Chuck Hauser

BLADEN COMMUNITY COLLEGE
Dublin, NC
Primary System Administrator: David Gooden

BLUE RIDGE COMMUNITY COLLEGE
Flat Rock, NC
Primary System Administrator: John Grice

BRUNSWICK COMMUNITY COLLEGE
Supply, NC
Primary System Administrator: John Kirby

CALDWELL COMMUNITY COLLEGE & TECHNICAL INSTITUTE
Hudson, NC
Primary System Administrator: Kathy Gragg

CAPE FEAR COMMUNITY COLLEGE
Wilmington, NC
Director of Computer Services: David Chappell

CARTERET COMMUNITY COLLEGE
Morehead City, NC
Primary System Administrator: Janet Spriggs

CATAWBA VALLEY COMMUNITY COLLEGE
Hickory, NC
Primary System Administrator: Linda McDaniel

CENTRAL CAROLINA COMMUNITY COLLEGE
Sanford, NC
Director of Information Technology: Darrell Lewis

CENTRAL PIEDMONT COMMUNITY COLLEGE
Charlotte, NC
Primary System Administrator: Harold Walker

CLEVELAND COMMUNITY COLLEGE
Shelby, NC
Primary System Administrator: Phyllis Haynes

COASTAL CAROLINA COMMUNITY COLLEGE
Jacksonville, NC
Dean of Information Resources: Michael R. Dodge

COLLEGE OF THE ALBEMARLE
Elizabeth City, NC
Primary System Administrator: Sharon Fairchild

CRAVEN COMMUNITY COLLEGE
New Bern, NC
Director of Administrative & Computer
Services (Primary System Administrator): Deborah Joyner

DAVIDSON COUNTY COMMUNITY COLLEGE
Lexington, NC
Director, Information Systems Support Services: Terri Yates

DURHAM TECHNICAL COMMUNITY COLLEGE
Durham, NC
Director, Information Technology Services: Beverly McComb

EDGECOMBE COMMUNITY COLLEGE
Tarboro, NC
Primary System Administrator: Larry Stroud

FAYETTEVILLE TECHNICAL COMMUNITY COLLEGE
Fayetteville, NC
Assistant to the President for MIS: Dan Prescott

FORSYTH TECHNICAL COMMUNITY COLLEGE
Winston-Salem, NC
Director of Information Systems: Rick Newsome

GASTON COLLEGE
Dallas, NC
Director of Technology Services: Tim Wilson

GUILFORD TECHNICAL COMMUNITY COLLEGE
Jamestown, NC
Director of MITS: Sandie Kirkland

HALIFAX COMMUNITY COLLEGE
Weldon, NC
System Administrator: Sis Tucker

HAYWOOD COMMUNITY COLLEGE
Clyde, NC
System Administrator: Bruce Denton

ISOTHERMAL COMMUNITY COLLEGE
Spindale, NC
Primary System Administrator: Curtis Vance

JAMES SPRUNT COMMUNITY COLLEGE
Kenansville, NC
Coordinator Management Information
Systems/System Administrator: Gail Sapp

JOHNSTON COMMUNITY COLLEGE
Smithfield, NC
Primary System Administrator: Judy Davis

LENOIR COMMUNITY COLLEGE
Kinston, NC
Primary System Administrator: Gerry Fox

MARTIN COMMUNITY COLLEGE
Williamston, NC
Primary System Administrator: Martha Mosley

MAYLAND COMMUNITY COLLEGE
Spruce Pine, NC
Primary System Administrator: Dickie Perry

MCDOWELL TECHNICAL COMMUNITY COLLEGE
Marion, NC
Director of Technology/Information Systems: Elmer Macopson

MITCHELL COMMUNITY COLLEGE
Statesville, NC
System Administrator: Marie Prather

MONTGOMERY COMMUNITY COLLEGE
Troy, NC
Management Information Services: Teng Vang
(Primary System Administrator)

NASH COMMUNITY COLLEGE
Rocky Mount, NC
Primary System Administrator: Anne Hancock

PAMLICO COMMUNITY COLLEGE
Grantsboro, NC
Primary System Administrator: David Looney

PIEDMONT COMMUNITY COLLEGE
Roxboro, NC
Director Management Information Systems: Phil Hille

PITT COMMUNITY COLLEGE
Greenville, NC
Primary System Administrator: Joseph Schuhbauer

RANDOLPH COMMUNITY COLLEGE
Asheboro, NC
System Administrator: Tara Williams

RICHMOND COMMUNITY COLLEGE
Hamlet, NC
Primary System Administrator: Chris Sturdivant

ROANOKE-CHOWAN COMMUNITY COLLEGE
Ahoskie, NC
Primary System Administrator: Gerald Harrell

ROBESON COMMUNITY COLLEGE
Lumberton, NC
Primary System Administrator: Judy Jones

ROCKINGHAM COMMUNITY COLLEGE
Wentworth, NC
Director of Technology Support Services: Dale O'Bryant

ROWAN-CABARRUS COMMUNITY COLLEGE
Salisbury, NC
Director, Administrative Computer Operations: Linda Hoffner

SAMPSON COMMUNITY COLLEGE
Clinton, NC
Computer Systems Administrator: Ronnie Bryant

SANDHILLS COMMUNITY COLLEGE
Pinehurst, NC
Director of Information Systems: Dorothy Savin

SOUTH PIEDMONT COMMUNITY COLLEGE
Polkton, NC
Director and System Administrator: Anna Baucom

SOUTHEASTERN COMMUNITY COLLEGE
Whiteville, NC
System Administrator: Sharon Mendenhall

SOUTHWESTERN COMMUNITY COLLEGE
Sylva, NC
Primary System Administrator: Elaine Estes

STANLY COMMUNITY COLLEGE
Albemarle, NC
Director of Technology: Ed Thomas

SURRY COMMUNITY COLLEGE
Dobson, NC
Assistant Vice President and System Administrator: Charles W. Strickland

TRI-COUNTY COMMUNITY COLLEGE
Murphy, NC
Primary System Administrator: Brian Wolf

VANCE-GRANVILLE COMMUNITY COLLEGE
Henderson, NC
Director of Information Technology: Darryl McGraw

WAKE TECHNICAL COMMUNITY COLLEGE
Raleigh, NC
Primary System Administrator: Herman Wright

WAYNE COMMUNITY COLLEGE
Goldsboro, NC
Primary System Administrator: Kathy Jones

WESTERN PIEDMONT COMMUNITY COLLEGE
Morganton, NC
Primary System Administrator: Nancy Norris

WILKES COMMUNITY COLLEGE
Wilkesboro, NC
Primary System Administrator: Tom Caudill

WILSON TECHNICAL COMMUNITY COLLEGE
Woodard Station Wilson, NC
Unix System Administrator: Janet Mintern

(IIPS Directory, August 27, 1999)

Appendix F:
Introductory Packet Materials

October 12, 2001

«Title» «FirstName» «LastName»
«JobTitle»
«Company»
«Address1»
«City», «State» «PostalCode»

Dear «Title» «LastName»:

The purpose of this letter is to invite you to participate in a research study that may assist educational leaders and benefit educational institutions within the North Carolina Community College System. You have exceptional expertise and knowledge concerning your college's information systems; therefore, I need and would appreciate your perspective and feedback.

The results of this study will be compiled in a dissertation as completion of my doctoral studies at Regent University. The research focuses upon computer ethics issues and the need for computer policies and instruction. The feedback provided by you and other key personnel across the NCCC system will be used to better understand computer user behavior, and to offer ethical guidance and assistance in an effort to reduce or eliminate current ethical dilemmas experienced by educational leaders.

The research materials that participants will receive consist of a computer ethics assessment survey of 15 questions, and a working model of a computer ethics policy with an instructional plan that you will be asked to evaluate on a brief response sheet. The entire packet should require only about 10 to 20 minutes to complete. Your responses will remain completely confidential and your name or college name will never be associated with your input. A stamped envelope will be enclosed in the packet to return the survey and response sheet.

Enclosed with this letter is a postcard to return indicating your willingness to participate in this study. Please note on the postcard your preference for receiving the materials and return immediately. Also enclosed with this letter is a summary statement explaining the purpose of the study.

Thank you so very much for your time and attention. I really appreciate your valuable information and input. Respondents will receive their materials within one to two weeks. A packet will also be mailed to those who choose not to respond for your information, and to offer an additional opportunity to participate in the study.

Sincerely,

Regina DeLisse
Coordinator Computer Science/Business
Wilkes Community College

Research Summary

The prominence of information technologies resulting in dependence on computers as necessary tools has penetrated all of society, including the education field and its institutions of higher learning. However, the speed at which technological advancements have progressed appears to have been far faster than consideration of their impact upon societal or cultural norms and values or the development of norms governing the use of the technologies. While utilizing and harnessing information technology of numerous types have brought various ethical issues, many of these have focused on and been unique to the Internet and its capacity to connect individuals, including those on college campuses, to the world.

While leaders in all fields have faced ethical dilemmas, educational leaders, including community college leaders, have struggled particularly with the increasing ethical demands of information technology. The basic dilemma for institutions of higher education is to find a way to satisfy the need for freedom of information access and dissemination and, at the same time, accommodate the various conflicting social values of their diverse communities.

One of the key factors in this study is the examination of computer user behavior. Individual behavior is a focus of study in an effort to develop and implement a more effective computer ethics policy. One behavioral theory that appears to offer a particularly promising framework for developing computer ethics policies, procedures and instruction on college campuses is the Theory of Deindividuation (Festinger, Pepitone, and Newcomb, 1952; Zimbardo, 1969). The basic premise of this theory suggests that when individuals are submerged within a group they become anonymous and lose conscious personality. This feeling of being unseen and not personally identifiable enables individuals to express primitive feelings and impulses, and possibly unethical behavior. The Internet and networked computers allow individuals to locate others with whom they may wish to identify. Recent studies have confirmed the connection between deindividuation and information technology.

This study focuses upon the community college, as opposed to other educational institutions, based upon the fact that the community college offers a unique opportunity for educational administrators to inform computer users. There is a need for research by scholars focusing upon the impact of information technology and clarity of ethical implications caused by computer usage. Based upon the growing importance of community colleges and the opportunity to reach a larger, more diverse student population, the issues within this educational system are worthy of further investigation.

The North Carolina Community College System may typify the need for computer ethics policies or better ones for community colleges and appears to have distinctive opportunities and implications for addressing organizational leadership issues. Statistically, it appears to be comparable to other state systems in all criteria: diverse student population, high enrollment numbers, societal impact, emphasis on business and industry, and reflection of the community it serves. A second factor, which provides the

North Carolina system with a symbolic role, is its commitment to respond to the changing demands of information technology. The resulting issues and concerns appear representative of similar college systems throughout the country.

Research is needed to help determine what community college leaders think about current problems and issues as well as viable solutions. There is a need for not only new research into the problem, but, given that most policies are fixed rules or codes that seem to be ineffective, there is a need to view and develop these policies using new theoretical perspectives. In addition to policies, implementation guidelines must be developed to assist educators in the provision of ethical instruction. Finally, research is imperative for closer scrutiny of the underlying principles and theoretical concepts that promote and facilitate ethical conduct by computer users.

Appendix G:
Research Packet Cover Letters

October 12, 2001

«Title» «FirstName» «LastName»
«JobTitle»
«Company»
«Address1»
«City», «State» «PostalCode»

Dear «Title» «LastName»:

Thank you for your willingness to participate in this study. The valuable input that you will provide will be used to assist and inform educators regarding computer user behavior and how to reduce or eliminate unethical conduct.

The working model of the computer ethics policy is based upon an analysis of a random sampling of 50 existing computer policies from universities and community colleges across the nation. In addition, the use of Wilkes Community College in the computer policy and instructional plan are for demonstration purposes only and do not constitute an existing agreement. Use of this name is merely to demonstrate how a particular community college might utilize such materials.

To compile your information the following materials have been included:

- NCCCS Computer Ethics Assessment Survey
- WCC Computer Ethics Policy
- WCC Guidelines for Appropriate Computing Behavior
- Policy and Instruction Response Sheet.

Please return only the NCCCS Computer Ethics Assessment Survey and Policy and Instruction Response Sheet at your earliest convenience. The other two documents may be disposed of and do not need to be returned. If you would be interested in obtaining a copy of the final results please indicate on the return Policy and Instruction Response Sheet. Thank you again for your assistance.

Sincerely,

Regina DeLisse
Coordinator Computer Science/Business
Wilkes Community College

October 12, 2001

«Title» «FirstName» «LastName»
«JobTitle»
«Company»
«Address1»
«City», «State» «PostalCode»

Dear «Title» «LastName»:

The materials contained in this packet are provided for your personal information. As I indicated in my original letter, this is also an additional invitation to participate in the research effort. You have more knowledge about computer issues than anyone else on your campus; your input, thus, would be helpful in informing other educators about computer user behavior and developing guidelines for ethical computer conduct. A computer ethics policy and ethical education can instruct students how to behave more ethically and may encourage accountability as they use college computing services. Perhaps the work will also reduce the effort and expense system administrators incur because of unethical student computer activity. It is clear that a comprehensive computer ethics policy and instruction are very inexpensive when compared to other measures currently used to monitor, filter and regulate student computer use.

The working model of the computer ethics policy is based upon an analysis of a random sampling of 50 existing computer policies from universities and community colleges across the nation. In addition, the use of Wilkes Community College in the computer policy and instructional plan are for demonstration purposes only and do not constitute an existing agreement. Use of this name is merely to demonstrate how a particular community college might utilize such materials.

To compile your information the following materials have been included:

- NCCCS Computer Ethics Assessment Survey
- WCC Computer Ethics Policy
- WCC Ethical Instruction Plan
- Policy and Instruction Response Sheet.

Please return only the NCCCS Computer Ethics Assessment Survey and Policy and Instruction Response Sheet at your earliest convenience. The other two documents may be disposed of and do not need to be returned. The survey and response sheet may be printed, completed then returned by FAX at (336) 246-5943, or scanned in and e-mailed at delisse@SkyBest.com or delisser@gw.wilkes.cc.nc.us. If you have any questions or concerns, please feel free to contact me at (336) 246-3900, (828) 265-3531, or e-mail. Thank you again for your assistance.

Sincerely,

Regina DeLisse
Coordinator Computer Science/Business
Wilkes Community College

October 12, 2001

«Title» «FirstName» «LastName»
«JobTitle»
«Company»
«email»

Dear «Title» «LastName»:

I sincerely appreciate the time and attention that you are giving to this research project. I apologize for any inconvenience returning the materials. It has come to my attention that we are experiencing problems with our FAX machine. As a result, I am mailing a postage paid return envelope to you. If by chance you also need another copy of the research materials, please e-mail me at delisse@skybest.com or delisser@gw.wilkes.cc.nc.us and I shall send those promptly.

Thank you again for your insight and input concerning this study.

Sincerely,

Regina DeLisse
Coordinator Computer Science / Business
Wilkes Community College

Appendix H:
Research Packet Materials

North Carolina Community College System
Computer Ethics Assessment Survey

Section I. Please circle the number indicating your best response to the following questions.

1. How often have you experienced occurrences of computer users (students, faculty, staff) on your college campus:

sharing user access or passwords, stealing passwords, or unauthorized accessing data?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

showing a lack of respect for the privacy and security of other users, data, or network system?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

using computing resources for purposes other than those specified or originally intended.

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

using computing resources for personal gain?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

monopolizing resources (playing games); wasting software, hardware, or supplies?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

using computing resources to commit crimes; theft or destruction of hardware and/or software?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

engaging in software piracy, illegally copying of licensed software, or infringing upon software license agreements?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

knowingly transmitting or creating computer viruses?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

intercepting transmitted information, hacking into networks and systems, or cracking codes either on campus or from another location?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

engaging in the displaying, downloading, and viewing of inappropriate, offensive or obscene materials?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

engaging in the transmission of obscene, defamatory, harassing, offensive, annoying, or abusive e-mails?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

misrepresenting the college on the Internet or falsifying their identity?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

posting information on the Internet that violates the college code of conduct?

5	4	3	2	1
Frequently	Occasional	No Opinion	Seldom	Never

2. What additional inappropriate uses of computers have you experienced or are aware of at your college?

3. What steps, precautions, or measures has your campus taken to resolve problems such as indicated in the preceding questions? How effective have these measures been? (use back of sheet if necessary)

Section II. Please circle the number indicating the extent to which you agree or disagree with the following statements.

4. Ethical problems have increased since our campus provided connection to a local area network and Internet as opposed to providing just stand alone PCs and general computer lab use.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

5. Ethical use of computers is becoming a critical issue that needs to be addressed at our college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

6. Student use of computers and the Internet have had a positive impact on our college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

7. Student uses of computer chat rooms have created safety issues or concerns for our college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

8. Unlike students, the faculty and staff rarely contribute to ethical problems relating to computing resources at my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

9. A computer ethics policy is important for the protection of the mission and purpose of our college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

10. The fact that computer users can remain anonymous on the Internet may have led to a number of unethical computer usage incidents at our college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

11. Computer users at our college use computers in ways that they would normally not because there is less likelihood of getting caught.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

12. The Internet increases the occurrence of unethical and antisocial behavior because computer users in our labs can easily identify others exhibiting similar unethical and/or antisocial behaviors.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

13. My college has an existing computer ethics policy for all computer users (acceptable use policy, or similar wording).

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

14. The reason my college does not have a suitable computer ethics policy is due to a lack of time and resources to create or modify one.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

15. A computer ethics policy and ethics instruction at our college would increase ethical and prosocial behavior because users would identify with appropriate behavior.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

Wilkes Community College
Computer Ethics Policy

As stated in the college handbook the purpose statement of Wilkes Community College is:

> As a public, two-year, "open door" institution, Wilkes Community College is committed to providing comprehensive education and educational support services for people in Wilkes, Ashe, and Alleghany counties and the surrounding region. As a member of the North Carolina Community College System, the college seeks to enhance economic, cultural, and social development by providing
>
> - Quality education, training and retraining for the workforce, including basic skills education, occupational, technical, and pre-baccalaureate programs;
> - Support for economic development through services to business and industry, both public and private; and
> - A variety of services and cultural activities that improve the quality of life.
>
> (WCC Handbook, 1999-2000).

Preamble: In upholding and promoting the mission of Wilkes Community College, it is assumed that certain basic values will advance this purpose. These values are the foundation for this computer ethics policy. They include facilitating and encouraging the highest level of scholarship and leadership and eliciting the highest standards of honesty, integrity, and academic excellence among all persons associated with and interested in Wilkes Community College.

I. Policy Purpose

The primary purpose of the Wilkes Community College Computer Ethics Policy is to empower students to make the wisest and most ethical decisions when faced with information technology related dilemmas. As part of the educational endeavor and in accordance with the mission statement of Wilkes Community College, this policy is set forth for the development of individual character within the computing environment.

The secondary purpose of the Computer Ethics Policy is to ensure the integrity of both hardware and software of Wilkes Community College and to maintain the basic mission of the college in teaching and learning. The college relies heavily upon computing resources to meet operational, financial, educational, and informational needs; it is essential that the systems are protected from misuse and unauthorized access.

Utilizing and accessing the college's computing resources is a privilege provided to all computer users (faculty, staff, and students). All users have an obligation to behave in a responsible, ethical, and legal manner. The same moral and ethical behavior expected outside the computing environment also applies within the computing environment.

This agreement constitutes a legally, ethically, and technically valid document. In addition to this computer ethics policy, users are subject to applicable state and federal laws.

II. Guidelines for Appropriate Computing Behavior

Integrity and Accuracy

Actions altering or interfering with the intended use and purpose of college computing resources constitute inappropriate and unethical computing behavior. Examples of inappropriate and unethical behavior include:

- sharing user access or passwords, stealing passwords, or unauthorized accessing data
- using computing resources for purposes other than those specified or originally intended
- using computing resources for or using resources for personal

gain

- knowingly transmitting or creating computer viruses
- intercepting transmitted information, hacking into networks and systems, or cracking codes either on campus or from another location

Copyright and Licensing

All users and policy administrators of the college are expected to comply with copyright laws and licensing agreements. All software must be in full compliance with proper licensing agreements. Examples of unethical behavior concerning piracy and copyright issues include:

- engaging in software piracy, illegally copying of licensed software, or infringing upon software license agreements
- loading, downloading from any source, copying or borrowing software that is in violation with existing licensing or laws
- knowingly alter software belonging to the college that violates copyright laws and licensing agreements

Users violating copyright laws and licensing agreements will be held responsible and legally liable for damages and penalties imposed. As a revision to the existing copyright law, users may borrow small amounts of printed, audio, or video materials constituted as "fair use." This use is for purposes of "criticism, comment, news reporting, teaching, scholarship or research" (Copyright Revision Act, p 16). What is considered "fair use" is subject to college approval.

Privacy

All individual users are guaranteed a right to privacy of intellectual materials that are academically and educationally related. Examples of inappropriate and unethical computing behavior relating to privacy issues include:

- showing a lack of respect for the privacy and security of other users, data, or network system
- borrowing, copying, examining, or removing another user's electronic mail, files, records, passwords, or personal property

Damages and Material Usage

Users are required to respect the college's computing facilities. Abuses of software, hardware, related media, equipment and supplies may result in the temporary or permanent suspension of the user. In some cases, users may be held legally liable for damages, repairs, and/or replacements. Examples of unethical behavior concerning damages and material usage include:

- monopolizing resources (playing games); wasting software, hardware, or supplies
- using computing resources to commit crimes; theft or destruction of hardware and/or software

Internet and Electronic Mail

All users are to respect and properly represent the college, faculty, staff, student body, and community at all times while connected to the Internet or college networking system. Examples of unethical behavior regarding the Internet and e-mail include:

- engaging in the displaying, downloading, and viewing of inappropriate, offensive or obscene materials
- downloading shareware without compliance to payment and registration, or freeware that is permanently installed on the computer hard drive
- engaging in the transmission of obscene, defamatory, harassing, offensive, annoying, or abusive e-mails
- misrepresenting the college on the Internet or falsifying their identity
- posting information on the Internet that violates the college code of conduct

Users must avoid vulgar or offensive language, and regard on-line systems with consideration and respect. Users must also be mindful of the importance of using connection time and equipment wisely.

III. Liability

The college may take disciplinary or legal action against any individual in violation of this computer ethics policy. This action may result in the temporary or permanent suspension of user privileges or computing facilities. Severe cases may require the suspension or permanent separation of the individual from the college. The college expressly and explicitly disclaims any liability and/or responsibility for violations of the policy as stated herein.

IV. Student Contract

I have read and agree to abide by the terms and conditions of the Wilkes Community College Computer Ethics Policy, and as such I am granted all the rights and privileges of computer use associated with this agreement by Wilkes Community College. I accept full responsibility for failure to comply with any or part of this agreement, and I acknowledge that willful misconduct and failure to maintain this contract may result in actions by Wilkes Community College. Actions may include fines for damages, temporary or permanent suspension of user rights, disciplinary actions as deemed necessary, and legal actions caused by failure to comply with copyright laws and licensing agreements.

Signature **Date**

Wilkes Community College
Ethical Instruction Plan

This guideline for appropriate computing behavior and ethical conduct consists of a sixteen week instructional plan for introducing ethical topics for class discussion. This module may be included within any existing computer course; however, an introductory computer course may be preferable. Each topic is introduced by the instructor and followed by class discussion. Each point listed below comes from the college's computer ethics policy. While students should have already read the policy and signed their student contract at the beginning of the semester, they may not fully understand all the ethical issues outlined in the policy. The purpose of this instructional unit is to provide students with an understanding of why ethical behavior is necessary and how to make the wisest decisions when faced with ethical dilemmas.

Ethical cases are provided by Oz's (1994) "Ethics: for the Information Age." According to Oz research shows that one of the most effective methods to teach ethics is to stimulate individual thinking and personal interpretation through the case based approach. The ethical cases place students in dilemmas that each must solve alone. There are no right or wrong answers provided with the cases; however, Oz does recommend using the utilitarian approach for the greatest good for the greatest number of people. While the class discussion topics are ordered, the ethical cases are in no direct order and may be arranged to suit individual instructor preferences.

Integrity and Accuracy

- Week 1: sharing user access or passwords, stealing passwords, or unauthorized accessing data
- Week 2: using computing resources for purposes other than those specified or originally intended
- Week 3: using computing resources for personal gain
- Week 4: knowingly transmitting or creating computer viruses
- Week 5: intercepting transmitted information, hacking into networks and systems, or cracking codes either on campus or from another location

Copyright and Licensing

- Week 6: engaging in software piracy, illegally copying of licensed software, or infringing upon software license agreements
- Week 7: loading, downloading from any source, copying or borrowing software that is in violation with existing licensing or laws
- Week 8: knowingly altering software belonging to the college that violates copyright laws and licensing agreements

Privacy

- Week 9: showing a lack of respect for the privacy and security of other users, data, or network system

- Week 10: borrowing, copying, examining, or removing another user's electronic mail, files, records, passwords, or personal property

Damages and Material Usage

- Week 11: monopolizing resources (playing games); wasting software, hardware, or supplies; using computing resources to commit crimes; theft or destruction of hardware and/or software

Internet and Electronic Mail

- Week 12: engaging in the displaying, downloading, and viewing of inappropriate, offensive or obscene materials
- Week 13: downloading shareware without compliance to payment and registration, or freeware that is permanently installed on the computer hard drive
- Week 14: engaging in the transmission of obscene, defamatory, harassing, offensive, annoying, or abusive e-mails
- Week 15: misrepresenting the college on the Internet or falsifying their identity
- Week 16: posting information on the Internet that violates the college code of conduct

Ethics Cases:

1. Luddonia And Summonia
2. Data Alteration
3. Worker Displacement
4. Monitoring E-Mail
5. Conflicts And Priorities
6. Obligations To Clients
7. High-Tech Diagnosis
8. Obligations To Employer
9. Miscommunications
10. Ethics In Higher Education
11. Ethics In Politics
12. Invasion Of Privacy
13. Fraud And Money Theft
14. First Amendment Rights
15. Obligations To Society
16. Confidentiality

Policy and Instruction
Response Sheet

Please read and respond to the two illustrative documents: the Computer Ethics Policy and the Ethical Instruction Plan. In responding, please answer the statements below in terms of your personal preference and needs of your particular community college. The primary purpose of this response sheet is to gain valuable insights from you regarding a policy and plan that would be beneficial to North Carolina community colleges, and to determine how the policy may be modified to suit individual colleges.

1. It is appropriate for a computer ethics policy to open with the college's mission statement.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

2. The policy purpose appears to need no additional information or explanation.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

3. Additional information needed in the policy purpose for my college is:

____

____

____

____

4. Components listed in the Guidelines for Appropriate Computing Behavior cover all the major ethical issue areas and no additional sections are needed.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

5. Additional sections necessary for my college would be:

____

____

____

____

6. A computer ethics policy should be applicable to all users rather than just students.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

7. Explaining what constitutes unethical behavior appears to be best conveyed through listing examples in the policy.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

8. The liability section is needed, but would require revisions for my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

9. Revisions to the liability section for my college would include:

____

____

____

____

10. The student contract is a necessary component in order to make students accountable for their behavior at my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

11. Student signatures on a contract probably would have very little impact on their behavior at my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

12. Faculty and staff at my college should be bound to the policy although not required to sign a contract.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

13. A computer ethics policy will most likely reduce or eliminate unethical behavior at my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

14. The ethical instrúction plan appears relevant and necessary to increase ethical behavior at my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

15. Students probably would not understand the computer ethics policy without the instructional plan.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

16. Students probably would not abide by a computer ethics policy without computer ethics instruction.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

17. Instructors at my college would be receptive to spending class time teaching ethics.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

18. An ethics component should be included in all computer classes at my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

19. Many computer users act unethically at my college simply because they do understand how to behave ethically.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

20. Many users understand ethical conduct, but feel they can escape detection at my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

21. The signed student contract should be considered a legal document and would reduce liability issues at my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

22. The fact that students sign a contract would make them feel more identified and cause them to behave more ethically at my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

23. Students should be given an access number or other means of tracking, because the contract alone is insufficient to reduce unethical behavior.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

24. Computer users at my college would behave more ethically if they perceived that they could be monitored during computer usage in our labs.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

25. Computer users at my college would behave more ethically if they perceived that they could be monitored during Internet usage in our labs.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

26. There is a connection between student anonymity and unethical behavior at my college; the presence of a computer ethics policy and signed contract would reduce their anonymity.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

27. A computer ethics emphasis similar to the model policy and instructional plan would benefit my college.

5	4	3	2	1
Strongly Agree	Agree	No Opinion	Disagree	Strongly Disagree

28. Additional suggestions or comments I would like to make are: (i.e.: what additional content might be added to the policy or plan; teaching methods; difficulties implementing a policy)

____

____

____

____

____

____

____

Appendix I:
Means and Standard Deviations:
Arranged by Research Questions

Table 15

Means and standard deviations for question 1a-m

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Q1A	18	2.00	5.00	3.7222	1.0178
Q1B	18	2.00	5.00	3.1111	1.1827
Q1C	18	2.00	5.00	4.0556	.8726
Q1D	18	1.00	5.00	2.7778	1.3086
Q1E	18	2.00	5.00	3.6667	.9701
Q1F	18	1.00	4.00	1.6111	.9785
Q1G	18	1.00	4.00	2.7222	1.2274
Q1H	18	1.00	4.00	1.4444	.9835
Q1I	18	1.00	4.00	1.5556	.7838
Q1J	18	1.00	5.00	2.8889	1.1827
Q1K	18	1.00	4.00	2.0556	.9984
Q1L	18	1.00	3.00	1.2778	.5745
Q1M	18	1.00	3.00	1.2778	.5745
Valid N (listwise)	18				

Table 16

Increase of technology-related ethical issues and impact of Internet usage

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Q4	18	2.00	5.00	3.6111	1.0922
Q6	18	4.00	5.00	4.5000	.5145
Q7	18	1.00	5.00	2.7778	1.1660
Valid N (listwise)	18				

Table 17

Colleges with an existing policy and importance of having a policy

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Q5	18	2.00	5.00	3.8333	.7859
Q13	18	2.00	5.00	4.1111	.9003
Valid N (listwise)	18				

Table 18

Limiting factors of colleges without a computer ethics policy

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Q14	18	1.00	4.00	2.7222	.8948
Valid N (listwise)	18				

Table 19

Alignment between mission of a college and a computer ethics policy

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Q9	18	4.00	5.00	4.4444	.5113
R1	15	2.00	5.00	3.8000	1.0823
Valid N (listwise)	15				

Table 20

Perception of an ethical component within college computer classes

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
R17	15	2.00	4.00	3.0667	.7988
R18	15	2.00	5.00	3.8000	.9411
Valid N (listwise)	15				

Table 21

Applicability of a computer ethics policy to all users (faculty, staff, and students)

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Q8	18	1.00	5.00	2.3889	1.0369
R6	15	4.00	5.00	4.8000	.4140
R12	15	1.00	5.00	3.7333	1.3345
Valid N (listwise)	15				

Table 22

Theory of Deindividuation usage to explain ethical behavior of computer users on community college campuses

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Q10	18	1.00	5.00	3.2222	1.0033
Q11	18	1.00	4.00	2.5556	1.1490
Q12	18	1.00	4.00	2.4444	.8556
R20	15	1.00	5.00	3.5333	1.0601
R24	15	4.00	5.00	4.2000	.4140
R25	15	4.00	5.00	4.2000	.4140
Valid N (listwise)	15				

Table 23

Utilization of the Theory of Deindividuation for developing computer ethics policies and instruction

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Q15	18	1.00	5.00	3.4444	1.0416
R7	15	2.00	5.00	4.0667	.7988
R26	15	2.00	5.00	3.6667	.7237
Valid N (listwise)	15				

Table 24

Potential of elements of the Theory of Deindividuation to be embedded in computer policies and instruction

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Q15	18	1.00	5.00	3.4444	1.0416
R22	15	2.00	5.00	3.8667	.6399
R26	15	2.00	5.00	3.6667	.7237
Valid N (listwise)	15				

Table 25

Participants' input concerning the components to be included in a computer ethics policy

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
R2	15	2.00	4.00	3.6667	.7237
R4	15	3.00	5.00	3.9333	.4577
R7	15	2.00	5.00	4.0667	.7988
R8	15	2.00	5.00	3.4667	.9155
Valid N (listwise)	15				

Table 26

Necessity and benefits of a student contract component within the computer ethics policy

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
R10	15	2.00	5.00	3.9333	1.0998
R11	15	1.00	4.00	2.3333	.9759
R21	15	2.00	5.00	3.3333	.8997
R22	15	2.00	5.00	3.8667	.6399
R23	15	1.00	4.00	2.7333	1.0328
Valid N (listwise)	15				

Table 27

Effectiveness of a computer ethics policy in support of the Theory of Deindividuation

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
R13	15	2.00	4.00	3.2000	.9411
Valid N (listwise)	15				

Table 28

Evaluation of the ethical instructional plan

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
R14	15	2.00	5.00	3.2667	.9612
R15	15	2.00	5.00	2.5333	.9904
R16	15	1.00	5.00	2.8667	1.1872
R19	15	1.00	5.00	2.4667	.9904
Valid N (listwise)	15				

Table 29

Potential of the computer ethics policy and instructional plan to reduce unethical behavior and benefit the colleges

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
R27	15	2.00	5.00	3.9333	.7037
Valid N (listwise)	15				

Appendix J:
Appropriate Use Policy: Durham Technical Community College Computing Resources

Appropriate Use Policy: Durham Technical Community College Computing Resources[1]

Durham Technical Community College provides a variety of computing resources to faculty, staff, students, and (in some cases) other members of the public. The appropriate use of these resources, including personal computers servers, networks, data sets, printers, Internet access, and software are the subject of this policy.

The College's Rights

The College owns most of the computers and all of the internal computer networks used on the campus. The College has the rights to the software and information residing on, developed on, or licensed for these computers and networks. The College has the right to administer, protect, and monitor this collection of computers, software, and networks. The College has the right to establish standards for security, privacy and data integrity on its computing systems as it deems appropriate. Furthermore, the College may determine the nature and extent of access to computer resources, may deny individuals access to computer systems and networks, and may determine who may connect a device to the computer system and the specifications for such a device.

The Individual's Responsibilities

1. **Use these computers for instruction, research, learning, and administration only.** Durham Tech's computers are for Durham Tech's use. They may not be used for outside business projects or personal activities.

2. **Respect licensing and copyright laws.** All software installed or used on Durham Tech computers must be legally licensed for use on the college premises. Do not copy copyright software from computers on campus or install software on campus computers that is not legally licensed. Licenses for software purchased by Durham Tech will be kept on file in the ITSD area. All other software licenses obtained by faculty and staff must be maintained by that user and produced upon request for verification. This includes all software including but not limited to freeware, shareware, and complementary software provided to faculty. Students are not allowed to load software unless under the direction of the faculty of staff.

3. **Maintain secure passwords.** Account passwords may not be shared with anyone, except instructors in certain cases. Use valid passwords that include at least one non-letter character and change them at last every four months.

4. **Protect College computer facilities.** Users are expected to abide by all federal and state laws governing computer use.[2] Users may not attempt to evade, disable or "crack" passwords or other security provisions. Also, users may not knowingly install any virus or destructive computer program onto campus computers.

Other Limitations and Warnings

1. **Resource limits may be imposed on all systems.** Users must abide by any resource limits set.

2. **Privacy is not guaranteed.** While there are technical and administrative policies in place that should protect computer information, computer data security is never perfect.

    - Unauthorized computer users may be able to breach security restrictions and gain access to your files.
    - Misdirected e-mail is not uncommon. Your e-mail messages may be seen by unintended recipients at Durham Tech or elsewhere on the Internet. If e-mail is considered confidential it should be sent by other means.
    - Systems administrators and other staff members may require access to files on any Durham Tech computers to perform audits or resolve technical problems. The College has the right to monitor E-mail transmission over its internal computer network. Legal mandates regarding confidentiality will be observed by computer staff when accessing data files.

3. **Users are responsible for backing up their data.** Users are responsible for backing up their own data files unless told that backup services are provided for their system.

Sanctions

Anyone who violates this policy is subject to the College's student code of conduct, the employees' due process policy, and possible criminal complaint or civil action for damages.

---

[1] Approved by the Durham Technical Community College Board of Trustees, July 1998.

2 It is a violation of federal and/or state criminal status for a person to knowingly access or attempt to access, a computer, computer system, computer network or any part thereof, for the purpose (i) devising or executing any scheme or artifice to defraud; (ii) services by means of false or fraudulent pretenses, representations or promises; (iii) unauthorized access; (iv) altering, damaging or destroying either computer hardware, software, or data; (v) without authorization, denying or causing the denial of computer system services to any authorized user of such computer system services; (vi) transmitting a computer virus with the intent to cause damage; (vii) transmitting without proper authorization a program, information, code or command with reckless disregard of a substantial and unjustifiable risk that the transmission will cause damage; or (viii) trackfficking in passwords with the intent to defraud. In many cases such violations are felonies and carry penalties of up to ten years in prison [18 U.S.C. 1030; N.C. Gen. Stat. 14-453 to 14-456.

Appendix K:
Computer Ethics Syllabi Samples

Sample I
"http://www.nd.edu/~rbarger/capp471syl.html"

UNIVERSITY OF NOTRE DAME

ELECTRONIC INFORMATION PROCESSING: STUDYING COMPUTER ETHICS, THE INTERNET, & THE WEB

Copyright (C) 1994 - 1998 by Robert N. Barger

- General information about the course
- Assignment descriptions and course requirements
- Assignment and exam calendar
- Tentative outline of the course
- Material about Computer Ethics
- The World Wide Web
- XML, HTML, & PUSH
- Additional on-line resources
- Recognition for this site

Course Description:
Students will study computer ethics, will learn several UNIX utilities, and such Internet applications as e-mail, listserv, telnet, ftp, newsgroups, talk, search engines, and the World Wide Web (including an introduction to HTML). Internet topics will be demonstrated on-line. Homework assignments and ethics case analyses will also be submitted on-line. The course is open to on-campus students who have a second major in Computer Applications. It can be used as an ethics or an applications course in the CAPP major requirements, but not as both.
Classroom & Time:
DeBartolo Hall 129; Tuesday & Thursday, 12:30 - 1:45 p.m.

Instructor:

Dr. Robert N. Barger, Computer Applications Faculty, Office: G126 Hesburgh Library, e-mail (from any N.D. UNIX host): rbarger (or from any Internet connection): rbarger@nd.edu Home Phone: (219) 289-8939, Office Phone: (219) 631-7459, Fax: (219) 631-8700. Note: Dr. Barger does not maintain set office hours, but welcomes contact either through e-mail or at his home phone.

Additional resource persons:

Guest network professionals (hereafter called NetPros) will participate in the class, usually by means of e-mail and listserv contributions. Many of the computer ethics cases provided in the section of this syllabus on computer ethics were contributed from the real life experiences of these professionals. This semester the NetPros will be Spenser Aden, Technical Director, NewOrder Media, Inc. in Nashville, Tennessee (Spenser_Aden@NOSPAMneworder.com); John Halleck, Computer Programmer and Administrator at the Academic Computing Library Information Services of the University of Utah, Salt Lake City, Utah (John.Halleck@NOSPAMcc.utah.edu); and Thomas Lapp, Senior Engineer, Computer Sciences Corporation, Newark, Delaware (thomas@NOSPAMmenno.com). Note: When using one of the above-mentioned e-mail addresses for the NetPros, first remove the letters "NOSPAM" from the address (it is included here to prevent spammers from collecting usable addresses over the Web).

Computer Assistance:

Help Desk, Room 111 Computing/Math Bldg., (219) 631-8111, info.1@nd.edu

Required Textbooks:

M. Ermann, M. Williams, & M. Shauf, COMPUTERS, ETHICS, AND SOCIETY (New York and Oxford: Oxford University Press, 1997).

Valerie Quercia, THE INTERNET IN A NUTSHELL (Sebastopol, CA: O'Reilly & Associates, Inc., 1997).

Recommended On-line Resources:

Lawrence Hinman, University of San Diego, ETHICS UPDATES

The Markkula Center for Applied Ethics, THE ETHICS CONNECTION

Click here for COURSE REQUIREMENTS AND GRADE WEIGHTING

Click here for ASSIGNMENT AND EXAM CALENDAR

Tentative Outline of Course Topics:

(Readings indicated in the textbooks, and links appearing in capital letters below, are required reading for the class.)

If any of the following Web links prove to be outdated or dysfunctional, please report them by e-mail to rbarger@nd.edu

1. Jan 13: Introduction to the course (overview of topics to be covered, explanation of assignments and grading procedure, SURVEY OF STUDENTS' INTERNET EXPERIENCE.
2. Computer Ethics (selected chapters in Ermann)
   - READING ASSIGNMENTS AND CLASS ACTIVITIES FOR COMPUTER ETHICS MATERIAL:
     - Jan 15: Ermann Ch 1; Videotape on Computer Ethics
     - Jan 20: Barger p 1 (Systems); Survey of students' philosophical & psychological beliefs
     - Jan 22: Interpretation of Philosophy survey scores; Barger p 2

        (Idealism)
        - Jan 27: Ermann Chs 5, 9, 24; Barger p 3 (Realism)
        - Jan 29: Barger pp 3-5 (Pragmatism); Ermann Ch 4
        - Feb 3: Barger pp 5-7 (Existentialism & Logical Analysis)
        - Feb 5: Ermann Ch 31;
          Click here for John Haas, 'THINKING ETHICALLY ABOUT TECHNOLOGY' [Natural Law approach];
          Click here for R. Barger,'A META-ETHICAL ANALYSIS OF COMPUTER ETHICS';
          Click here for IS COMPUTER ETHICS UNIQUE?
        - Feb 10: Click here for R. Barger, 'IN SEARCH OF A COMMON RATIONAL FOR COMPUTER ETHICS';
          Ermann Ch 35, pp 337-340
        - Feb 10: Click here for AN ECLECTIC APPROACH TO ETHICAL PROBLEM SOLVING , from the Markkula Center for Applied Ethics
        - Feb 10: 1st ethics case analysis due (Idealism)
        - Feb 12: Click here for a summary of R. Barger, 'KOHLBERG'S STAGES OF MORAL DEVELOPMENT'
        - Feb 12: Summaries of Keirsey's Four Temperaments:
          Rationalist 7 out of 42
          Idealist 20 out of 42
          Guardian 9 out of 42
          Artisan 6 out of 42
        - Feb 17 (review): Ermann Chs 32 & 33;
          Click here for a R. Barger, 'THUMBNAIL SUMMARY OF ETHICAL POSITIONS' in English, in Spanish, and in French
        - Feb 19: Exam on Computer Ethics

    - Click here for a SELECTION OF CASES TO BE USED FOR ETHICS ANALYSES

3. What is the Internet (Quercia, Ch 1, esp btm of p 13 about Cookies)
    - Feb 24: Click here for A DESCRIPTION OF THE INTERNET
    - Feb 24: Click here for MAP OF U.S. INTERNET SERVICE PROVIDERS
    - Feb 24: Click here for INTERNET DOMAIN SURVEY
    - Feb 24: Click here for INTERNET TOP LEVEL DOMAIN COUNTRY CODES
4. How the Internet Works (Quercia, Ch 4)
    - Feb 24: Click here for Joel Cooper's GRAPHIC PRESENTATION ABOUT THE INTERNET. (Joel is a former NetPro for this course).
    - Feb 24: 2nd ethics case analysis due (Realism)
    - Feb 26: Click here for THE CLINTON ADMINISTRATION'S PROPOSAL FOR PRIVATIZING DOMAIN REGISTRY
5. What Is Allowed on the Internet
    - Mar 3: Click here for A DESCRIPTION OF COPYRIGHT "FAIR USE"

    STANDARDS
  - Mar 3: Click here for a link to the closest thing to a standard-setting body the Web hasTHE WORLD WIDE WEB CONSORTIUM
6. Electronic Mail: the "pine" mailer and "mailto:" (Quercia, Ch 10)
  - Mar 3: HOW TO USE THE PINE MAILER
  - Mar 3: Click here for E-MAIL ASSIGNMENT. Assignment due Mar 7 at noon.
  - Mar 5: Presentations: Peter Cesaro, Electronic Trading Systems; Jennifer Howlin, Teaching children responsible use of technology; Stephanie Smith, The Communications Decency Act; Monica Salazar, Effects of computers on the public in the future; Bryan Harkins, Ethical concerns of computing in the workplace
  - Mar 5: Click here for E-MAIL ADDICTION (JOHN MCPHERSON'S 'CLOSE TO HOME' CARTOON)
  - Mar 5: How to send mail through the Web with the "mailto:" protocol
7. Listservs (optional reading: Quercia, Ch 11)
  - Mar 5: Click here for information on the CAPP3801 CLASS-LIST
  - Mar 5: Click here for LISTSERV ASSIGNMENT. Assignment due Mar 19, 8:00 a.m.
8. UNIX Commands
  - Mar 17: Click here for BASIC UNIX COMMANDS, and some notes on memory size.
  - Mar 17: Click here for HOW TO CREATE A .SIGNATURE FILE AND A PERSONALIZED PROMPT.
  - Mar 17: Click here for A TUTORIAL ON HOW THE PICO FILE EDITOR WORKS
9. Remote Login (telnet) and Gopher (Quercia, Ch 8)
  - Mar 17: Click here for INSTRUCTIONS ON HOW TO TELNET
  - Mar 17: Once upon a time there was a protocol named "gopher"
    Notre Dame's Gopher (...sayonara after Mar 15, 1998!)
    The Library of Congress Gopher
  - Mar 17: Presentations: Genevieve Yep, Effect of increased use of computers on our environment; Rich Kizer; Tom Asci, Microsoft v. U.S. Dept. of Justice; Carey May, Telecommuting; Michael Silva, Apple vs. Microsoft: A Brief Study in Management
  - Mar 17: 3rd Ethics Case Analysis due (Pragmatism)
10. File Transfer: ftp (Quercia, Chs 16, 17, 18, & 19)
  - Mar 19: Presentations: Nancy Doris, Web Publishing; Bill Helman, PGP; Jason Franken, Multimedia Copyright Law; Maciej Mrugala, Internet gambling; Bob Flannery, Browser Accelerators
  - Mar 19: Click here for FTP ASSIGNMENT Assignment due Mar 23, 8:00 a.m..
11. Network News (Quercia, Ch 12)
  - Mar 24: Presentations: Matthew Remke, Internet Telephony; Drew Geary, The Future of Apple; Kevin Stuart, Hackers on the Internet; Emily Miller,

Internet Credit Card Privacy and Fraud; John Kavanaugh, Microsoft Front Page

- Mar 24: Click here for the NEWSGROUP TO ANNOUNCE NEW WEB PAGES
- Mar 24: Click here for NEWSGROUP ASSIGNMENT Assignment due Mar. 27.

12. Finding Someone (Quercia, Ch 7)
    - Mar 26: Presentations: Darren Picciano, Digital Cameras and the Internet; Patrick Fear, Year 2000 problem; Maryclare Kenney, Electronic Frontier Foundation; Kristen Bell, Internet v. Intra-nets; Nicole Hinostro, Kids on the Net
    - Mar 26: Click here for FINGER ASSIGNMENT Assignment due Apr. 3.
13. The "talk" application
    - Mar 26: Click here for INFORMATION ABOUT "TALK"
14. The World Wide Web (Quercia, Ch 2 & 6)
    - Mar 26: Click here for AN INTRODUCTION TO URLs
    - Mar 26: Click here for TUTORIAL ON USE OF SEARCH ENGINES
    - Mar 26: Click here for SEARCH ENGINE ASSIGNMENT . Due Apr. 20.
    - Mar 31: 4th Ethics Case Analysis due (Existentialism) Click here for a sample case analysis done from an Existentialist perspective
    - Mar 31: Click here for LUCENT TECHNOLOGIES' TEXT-TO-SPEECH SYNTHESIS
    - Mar 31: Click here for "VIRTUAL" ANATOMY ANIMATION WITH SOUND
    - Mar 31: Click here for FREE SHOCKWAVE PLUGINS
    - Mar 31: Click here for A CURRENCY CONVERTER, INCLUDING ARCHIVED RATES & FUTURE PROJECTIONS
    - Mar 31: Click here for A WEB PAGE LANGUAGE TRANSLATOR
    - Mar 31: Click here to rotate and re-shape an image with "NETRIS - WRITTEN IN JAVA"
    - Mar 31: Click here to SEND A FAX VIA THE INTERNET
    - Mar 31: Click here for GATEWAY TO INDIANA STATE GOVERNMENT UNITS (LICENSE PLATES, TAX FORMS, ETC.)
    - Mar 31: Click here for a free website tune-up at the WEB SITE GARAGE
    - Apr 2: Presentations: Melinda Sinclair, Internet Radio; Tony Marino, Voting Over the Internet; James Belden, History of the Computer Virus; Paul Chadwick, Ordering thru the Internet
    - Apr 2: Review for exam (exam is April 7)
    - Apr 2: Click here for THE VATICAN WEBSITE
    - Apr 7: Exam on Internet & Web Applications
      Click here for comments on GRADING ADJUSTMENTS FOR THE INTERNET & WEB EXAM
15. XML, HTML 4.0, & PUSH
    - Apr 9: Presentations: Kelly Nichols, Encryption; Rene Mitsui, Censorship on the Internet; Kassandra Hartman, Image map creation; Leon Stronsky,

Computers and Disabilities; Brian Fleck, Spamming on the Internet

- Apr 9: Click here for FREQUENTLY ASKED QUESTIONS ABOUT THE EXTENSIBLE MARK-UP LANGUAGE (XML) It is recommended that you print out and study pp. 4 thru 12 of this document for the Final exam (i.e., Questions A1 thru C5, omitting questions A8, A11, A12, C3 & C4 [read only the first paragraphs of C3 & C4].
- Apr 9: Click here for AN INTRODUCTION TO HTML 4.0 It is recommended that you print out and study a copy of this 6 page document for the Final exam.
- Apr 21: Presentations: Ernesto Villalobos, Electronic Commerce: Security Requirements; Joe DiPiazza, Software Piracy; Meghan DeNiro, Teaching & Learning Using the Web; Kelly Donohue, Shopping on the Internet; Jim Pilla, Expert Systems; Travis Korth, Differences Between pine, eudora and imap; Mark Mennel, Internet Security; Colleen Duffy, A History of the Internet
- Apr 23: Click here for Spenser Aden's (one of our NetPros) presentation on PUSH TECHNOLOGY It is recommended that you take notes on this presentation for the Final exam.
- Apr 28: Presentations: Brandan Lucas, Shareware abuse; Michael Mitchell, Telecommuting; Shawn Nigg, Internet2; David Notarangelo, Web Page Design Using Net Objects; Paul Rainey, COGEN 2000; Catherine O'Connor, Employees' Personal Use of Business Computers; Alison Bonn, Internet Cookies; Paul Langanki, Pornography on the Web
- May 4: Final Exam on XML, HTML 4.0, and PUSH TECHNOLOGY Click here for an ALTERNATIVE FOR THE FINAL EXAM

Additional on-line information resources:

- Click here for HTML PRIMER BY ERIC MEYER
- Click here to access a WEB PAGE VALIDATOR which will check for conformity to various levels of HTML standards
- Click here for CHANGES FROM HTML 3.2 TO HTML 4.0
- Click here for A WEB-REVIEW ON STYLE SHEETS
- Click here for W3C's HTML 4.0 SPECIFICATION, SECTION ON STYLE SHEETS
- Click here for STILL MORE ON STYLE SHEETS
- Click here for a LESSON ON "NETIQUETTE". Read sections of this lesson beginning with "Electronic Mail and Files" and ending with "World Wide Web" (You may omit the "telnet" section).
- Click here for "SavvySearch" an Internet parallel query engine
- Click here for a large collection of WWW search engines
- Click here for the Hotbot search engine which is able to search a broader range of pages than most other engines and also has more possibilities for refining a search
- Click here for an index of Internet resources (the December list)
- Click here for the Electronic Frontier Foundation (EFF) Extended Guide to the Internet
- Click here for the Info Scout Report

- Click here for an Introduction to JavaScript by Stefan Koch

Click here to return to Dr. Barger's homepage

Sample II

Open to registered Duke University
and approved inter-institutional students only

Time:	**Place:**	**Instructor:**
Thurs, 7-9:30 pm	220 Gray Building	Wendy Robinson

Why Ethics and the Internet?

The focus of Ethics and the Internet (E&I) is on us rather than on the technology itself. Why do we care about the Net? Do we still care about ethics today? But even more essentially, who *are* we, the "users" of the Internet? According to Cyber Dialogue, the *Industry Standard*, Nielsen NetRatings, and other sources, between 48.2 to 70.5 million people in the U.S., out of a population estimated at 196.4 million, have come online. (See also the *Industry Standard*'s metrics on Gen X Internet Use and more recent estimates that place the number of adult Americans online to anywhere from 35.3 million or 63 percent according to Cyber Dialogue to 92 million or 40 percent of Americans and Canadians over the age of 16 according to Nielsen.) We've been growing exponentially since 1993-94 with the introduction of commercial applications for the World Wide Web, a way of accessing the Internet with a graphical user interface (GUI).

What might we be losing or gaining as a society as we move from a brick-and-mortar conception of the world toward increasing comfort with virtuality? What might we be losing or gaining as human beings as we move from the physical world of atoms to, as Nicholas Negroponte by way of William Shakespeare might have it, a brave new digital world? If we've profoundly become identified with numbers (digits) -- how do we, those of us in this course, feel about that? What might be the implications of this desocialization or resocialization, this dehumanization or greater human potential perhaps wrought by technology at the dawn of the next millennium? These are some of the questions we'll explore this semester.

Course Structure

If you browse through the syllabus, you'll see that the course is divided into three unequal parts: 1) What is the role of technology in society today, 2) How is the Net challenging existing public policy and our legal system, and 3) What are the new cyber frontiers and their ethical implications? What, for that matter, is "cyberspace" and why should we care? What is cyberculture and are we necessarily members thereof?

To approach answers to these questions, we'll read a variety of materials including email, Web sites, articles, essays, primary legal material, and, yes, even books. But our texts won't be restricted to print. We'll view films and tapes, participate in interactive multimedia, listen to guest lecturers, and/or, depending on class interest, take a

Syllabus Sections:

Assignments
Course requirements and grading criteria

Schedule
Searchable semester calendar with weekly topics and highlighted important dates

Texts
Reading list with weekly links and agenda

Students (participants only)
E&I registered users, including the email addresses and phone numbers for past and present students and guests

Attendance
Class roster

Papers and Projects
Students upload term papers and Web projects to their own E&I publishing areas

Chat (participants only)
Virtual office hours and conversations with guests

Discussion (participants only)
Class message board, restricted to enrolled students

News
E&I-related news and research links

Introductory Form
The first of several questionnaires that will be posted over the semester

Included in the eBLAST Encyclopedia Britannica Internet Guide

Past Semesters:

Summer 1999

Spring 1999

Fall 1997 - Spring 1996

Wendy Robinson (wendy) wgrobin@duke.edu. Duke University, Department of Religion, Durham NC USA 27708 Phone: (919) 767-2131 FAX: (919) 767-1711
revised: 09/05/99

Appendix L:
Sample Computer Ethics Policies Examined

1. Appalachian State University
2. Baylor University
3. Brewton Parker College
4. Brown University
5. Cedar Crest College
6. Cornell University
7. Delaware Technical Community College
8. Duke University
9. East Tennessee State University
10. Eastern College
11. Georgetown University
12. Georgia State University
13. Humboldt State University
14. Iowa State University
15. James Madison University
16. Keene State College
17. Kentucky Wesleyan College
18. Lindenwood College
19. Mission College
20. North Carolina State University
21. Pennsylvania State University
22. Princeton University
23. Queen's University
24. Regent University
25. Rice University
26. Stanford University
27. Taylor University
28. Texas A & M
29. Trinity University
30. University of Alabama
31. University of Arkansas
32. University of California at Berkeley
33. University of California at Irvine
34. University of Colorado
35. University of Delaware
36. University of Florida
37. University of Idaho
38. University of Kentucky
39. University of Maryland
40. University of Michigan
41. University of North Carolina at Chapel Hill
42. University of North Carolina at Charlotte

43. University of North Carolina at Wilmington
44. University of Notre Dame
45. University of Washington
46. Virginia Polytechnic Institute and State University
47. Wake Forest University
48. Wayne State College
49. Western Carolina University
50. Yale University

Universities & Colleges	Mission Statement	Policy Purpose	Passwords	Appropriate Usage	Personal Gain	Viruses	Hacking/Unauthorized Access	Copyright	Software Licensing	Privacy	Monopoliz Resource
1. Appalachian State University		1	1	1	1		1	1	1	1	1
2. Baylor University			1					1	1	1	
3. Brewton Parker College		1	1	1				1	1		
4. Brown University		1	1		1		1	1	1	1	1
5. Cedar Crest College			1		1		1	1	1	1	1
6. Cornell University		1	1				1	1	1		
7. Delaware Technical Community College		1	1		1		1	1	1	1	1
8. Duke University		1		1	1						1
9. East Tennessee State University		1	1		1	1	1	1		1	
10. Eastern College			1					1	1	1	1
11. Georgetown University		1	1			1	1	1	1	1	1
12. Georgia State University	1	1	1	1	1			1	1	1	1
13. Humboldt State University	1	1	1	1				1	1	1	
14. Iowa State University			1		1	1		1		1	1
15. James Madison University		1		1	1		1	1	1	1	1
16. Keene State College	1	1	1	1	1	1	1	1	1	1	
17. Kentucky Wesleyan College			1		1	1	1	1	1	1	1
18. Lindenwood College				1	1						1
19. Mission College		1	1	1				1	1	1	1
20. North Carolina State University			1	1	1		1	1	1	1	1
21. Pennsylvania State University								1	1		
22. Princeton University		1	1	1	1		1	1	1	1	1
23. Queen's University						1	1				
24. Regent University		1	1			1		1	1		1
25. Rice University			1			1	1	1	1		
26. Stanford University		1	1		1	1	1	1	1	1	1

Universities & Colleges	Wasting Materials	Theft/Damage	Downloading – Internet	Harassing E-mails	Identity Falsification	Use of Behavioral E1amples	Liability Section / Disciplinary Measures	User Contract
1. Appalachian State University		1		1	1	1	1	
2. Baylor University				1			1	
3. Brewton Parker College		1	1	1				1
4. Brown University		1		1			1	
5. Cedar Crest College	1	1	1	1		1		
6. Cornell University			1	1	1	1	1	
7. Delaware Technical Community College			1	1	1	1	1	
8. Duke University			1	1		1		
9. East Tennessee State University		1					1	
10. Eastern College				1		1	1	
11. Georgetown University				1		1	1	
12. Georgia State University				1		1	1	
13. Humboldt State University				1	1	1	1	
14. Iowa State University				1				
15. James Madison University		1		1		1	1	
16. Keene State College		1		1			1	
17. Kentucky Wesleyan College	1			1	1	1	1	
18. Lindenwood College	1			1				
19. Mission College			1	1	1		1	
20. North Carolina State University				1	1		1	1
21. Pennsylvania State University								
22. Princeton University	1			1	1		1	
23. Queen's University				1			1	
24. Regent University	1			1			1	
25. Rice University		1	1	1	1			
26. Stanford University		1		1			1	

Universities & Colleges	Other
1. Appalachian State University	Definition of terms
2. Baylor University	
3. Brewton Parker College	Three signatures on contract: user, parent, teacher
4. Brown University	
5. Cedar Crest College	
6. Cornell University	University disclaimer
7. Delaware Technical Community College	
8. Duke University	Connects sexual harassment to downloading inappropriate materials from Internet
9. East Tennessee State University	
10. Eastern College	
11. Georgetown University	
12. Georgia State University	
13. Humboldt State University	Hyperlink document contents at beginning of policy
14. Iowa State University	
15. James Madison University	
16. Keene State College	Prohibits political use
17. Kentucky Wesleyan College	
18. Lindenwood College	
19. Mission College	Prohibits all illegal and malicious acts with PC
20. North Carolina State University	
21. Pennsylvania State University	
22. Princeton University	
23. Queen's University	
24. Regent University	
25. Rice University	
26. Stanford University	Lists System Administrator responsibilities

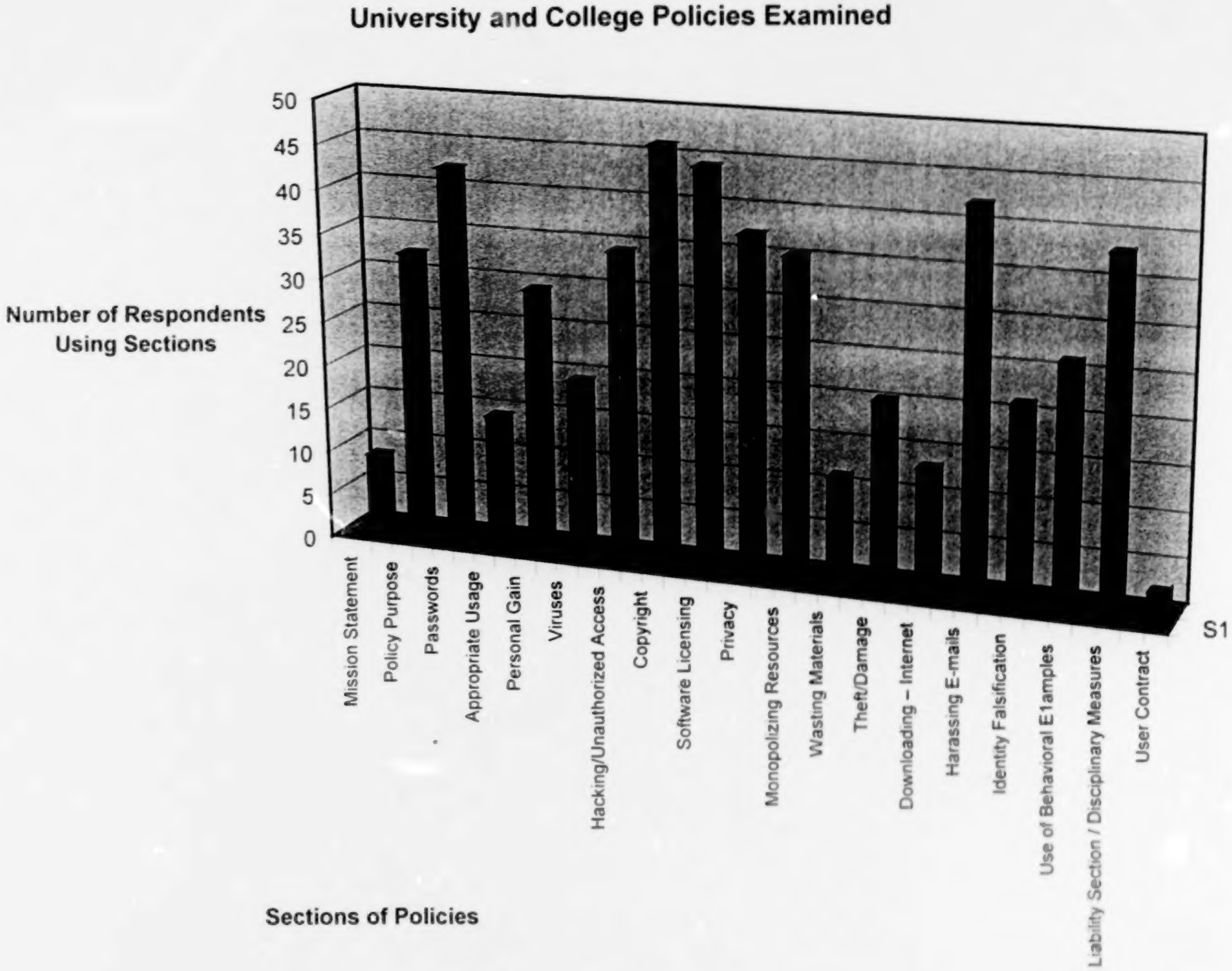
Universities & Colleges	Mission Statement	Policy Purpose	Passwords	Appropriate Usage	Personal Gain	Viruses	Hacking/Unauthorized Access	Copyright	Software Licensing	Privacy	Monopolizi Resource
27. Taylor University			1			1	1	1	1		1
28. Te1as A & M			1					1	1		
29. Trinity University	1		1		1	1	1	1	1	1	1
30. University of Alabama		1			1	1	1	1	1		1
31. University of Arkansas		1	1			1	1	1	1	1	1
32. University of California at Berkeley		1	1			1	1	1	1	1	1
33. University of California at Irvine		1	1		1	1	1	1	1	1	1
34. University of Colorado			1	1	1			1	1	1	1
35. University of Delaware	1	1			1		1	1	1	1	
36. University of Florida			1				1	1	1	1	1
37. University of Idaho		1	1		1		1	1	1	1	1
38. University of Kentucky	1	1	1		1	1	1	1	1	1	1
39. University of Maryland		1	1		1		1	1	1	1	1
40. University of Michigan	1	1	1			1		1	1	1	
41. University of North Carolina at Chapel Hill			1					1	1		
42. University of North Carolina at Charlotte							1	1	1		1
43. University of North Carolina at Wilmington		1	1		1			1	1	1	1
44. University of Notre Dame		1	1	1	1	1	1	1	1	1	1
45. University of Washington			1				1	1	1	1	
46. Virginia Polytechnic Institute and State University		1	1	1	1	1	1	1	1	1	1
47. Wake Forest University		1	1		1		1			1	
48. Wayne State College	1	1	1				1	1	1	1	1
49. Western Carolina University		1	1		1		1	1	1	1	1
50. Yale University		1	1		1		1	1	1	1	1
Totals	8	32	42	14	29	19	34	46	44	37	

Universities & Colleges	Wasting Materials	Theft/Damage	Downloading – Internet	Harassing E-mails	Identity Falsification	Use of Behavioral E1amples	Liability Section / Disciplinary Measures	User Contract

27. Taylor University			1	1		1	1	
28. Te1as A & M				1			1	
29. Trinity University		1		1	1	1		
30. University of Alabama	1			1				
31. University of Arkansas	1			1	1		1	
32. University of California at Berkeley	1	1		1	1	1	1	
33. University of California at Irvine	1	1		1	1	1	1	
34. University of Colorado		1	1	1	1	1	1	
35. University of Delaware		1					1	
36. University of Florida			1	1			1	
37. University of Idaho				1			1	
38. University of Kentucky	1				1	1	1	
39. University of Maryland		1	1		1	1	1	
40. University of Michigan				1		1	1	
41. University of North Carolina at Chapel Hill		1		1				
42. University of North Carolina at Charlotte						1	1	
43. University of North Carolina at Wilmington		1				1	1	
44. University of Notre Dame		1	1	1	1	1	1	
45. University of Washington				1	1			
46. Virginia Polytechnic Institute and State University	1			1		1	1	
47. Wake Forest University					1		1	
48. Wayne State College			1	1		1		
49. Western Carolina University		1		1	1	1	1	
50. Yale University		1		1	1	1	1	
Totals	11	20	13	42	21	26	38	2

Universities & Colleges	Other
27. Taylor University	
28. Te1as A & M	

29. Trinity University	
30. University of Alabama	
31. University of Arkansas	Prohibits use of chat programs
32. University of California at Berkeley	
33. University of California at Irvine	
34. University of Colorado	Addresses "Cyberculture"
35. University of Delaware	
36. University of Florida	
37. University of Idaho	
38. University of Kentucky	Has glossary
39. University of Maryland	
40. University of Michigan	
41. University of North Carolina at Chapel Hill	
42. University of North Carolina at Charlotte	
43. University of North Carolina at Wilmington	
44. University of Notre Dame	Has disclaimer and definition of terms
45. University of Washington	
46. Virginia Polytechnic Institute and State University	
47. Wake Forest University	
48. Wayne State College	Separate Internet Etiquette section
49. Western Carolina University	
50. Yale University	Elaborates on examples
Totals	


University and College Policies Examined
Number of Respondents Using Sections
50
45
40
35
30
25
20
15
10
5
0
Mission Statement
Policy Purpose
Passwords
Appropriate Usage
Personal Gain
Viruses
Hacking/Unauthorized Access
Copyright
Software Licensing
Privacy
Monopolizing Resources
Wasting Materials
Theft/Damage
Downloading – Internet
Harassing E-mails
Identity Falsification
Use of Behavioral E1amples
Liability Section / Disciplinary Measures
User Contract
S1
Sections of Policies

Appendix M:
Revised Model Computer Ethics Policy And Instructional Plan

Wilkes Community College
Computer Ethics Policy

As stated in the college handbook the purpose statement of Wilkes Community College is:

> As a public, two-year, "open door" institution, Wilkes Community College is committed to providing comprehensive education and educational support services for people in Wilkes, Ashe, and Alleghany counties and the surrounding region. As a member of the North Carolina Community College System, the college seeks to enhance economic, cultural, and social development by providing
>
> - Quality education, training and retraining for the workforce, including basic skills education, occupational, technical, and pre-baccalaureate programs;
> - Support for economic development through services to business and industry, both public and private; and
> - A variety of services and cultural activities that improve the quality of life.
>
> (WCC Handbook, 1999-2000).

Preamble: In upholding and promoting the mission of Wilkes Community College, it is assumed that certain basic values will advance this purpose. These values are the foundation for this computer ethics policy. They include facilitating and encouraging the highest level of scholarship and leadership and eliciting the highest standards of honesty, integrity, and academic excellence among all persons associated with and interested in Wilkes Community College.

I. Policy Purpose

The primary purpose of the Wilkes Community College Computer Ethics Policy is to empower faculty, staff, and students to make the wisest and most ethical decisions when faced with information technology related dilemmas. As part of the educational endeavor and in accordance with the mission statement of Wilkes Community College, this policy is set forth for the development of individual character within the computing environment.

The secondary purpose of the Computer Ethics Policy is to ensure the integrity of both hardware and software of Wilkes Community College and to maintain the basic mission of the college in teaching and learning. The college relies heavily upon computing resources to meet operational, financial, educational, and informational needs; it is essential that the systems are protected from misuse and unauthorized access.

Utilizing and accessing the college's computing resources is a privilege provided to all computer users (faculty, staff, and students). All users have an obligation to behave in a responsible, ethical, and legal manner. The same moral and ethical behavior expected outside the computing environment also applies within the computing environment.

This agreement constitutes a legally, ethically, and technically valid document. In addition to this computer ethics policy, users are subject to applicable federal, state and local laws.

II. Guidelines for Appropriate Computing Behavior

Integrity and Accuracy

Actions altering or interfering with the intended use and purpose of college computing resources constitute inappropriate and unethical computing behavior. Examples of inappropriate and unethical behavior include:

- sharing user access or passwords, stealing passwords, or unauthorized accessing data

- using computing resources for purposes other than those specified or originally intended
- using computing resources for or using resources for personal gain
- knowingly transmitting or creating computer viruses
- intercepting transmitted information, hacking into networks and systems, or cracking codes either on campus or from another location

Copyright and Licensing

All users and policy administrators of the college are expected to comply with copyright laws and licensing agreements. All software must be in full compliance with proper licensing agreements; all licensing agreements must be kept on file for auditing purposes. Examples of unethical behavior concerning piracy and copyright issues include:

- engaging in software piracy, illegally copying of licensed software, or infringing upon software license agreements
- loading, downloading from any source, copying or borrowing software that is in violation with existing licensing or laws
- knowingly alter software belonging to the college that violates copyright laws and licensing agreements

Users violating copyright laws and licensing agreements will be held responsible and legally liable for damages and penalties imposed. As a revision to the existing copyright law, users may borrow small amounts of printed, audio, or video materials constituted as "fair use." This use is for purposes of "criticism, comment, news reporting, teaching, scholarship or research" (Copyright Revision Act, p 16). What is considered "fair use" is subject to college approval.

Privacy

All individual users are guaranteed a right to privacy of intellectual materials that are academically and educationally related. Examples of inappropriate and unethical computing behavior relating to privacy issues include:

- showing a lack of respect for the privacy and security of other users, data, or network system
- borrowing, copying, examining, or removing another user's electronic mail, files, records, passwords, or personal property

Damages and Material Usage

Users are required to respect the college's computing facilities. Abuses of software, hardware, related media, equipment and supplies may result in the temporary or permanent suspension of the user. In some cases, users may be held legally liable for damages, repairs, and/or replacements. Examples of unethical behavior concerning damages and material usage include:

- monopolizing resources (playing games); wasting software, hardware, or supplies
- using computing resources to commit crimes; theft or destruction of hardware and/or software

Internet and Electronic Mail

All users are to respect and properly represent the college, faculty, staff, student body, and community at all times while connected to the Internet or college networking system. Examples of unethical behavior regarding the Internet and e-mail include:

- engaging in the displaying, downloading, and viewing of inappropriate, offensive or obscene materials
- downloading shareware without compliance to payment and registration, or freeware that is permanently installed on the computer hard drive
- engaging in the transmission of obscene, defamatory, harassing, offensive, annoying, or abusive e-mails
- misrepresenting the college on the Internet or falsifying their identity
- posting information on the Internet that violates the college code of conduct

Users must avoid vulgar or offensive language, and regard on-line systems with consideration and respect. Users must also be mindful of the importance of using connection time and equipment wisely.

III. Liability

The college may take disciplinary or legal action against any individual in violation of this computer ethics policy. This action may result in the temporary or permanent suspension of user privileges or computing facilities. Severe cases may require the suspension or permanent separation of the individual from the college and potential prosecution under federal, state, and local laws. The college expressly and explicitly disclaims any liability and/or responsibility for violations of the policy as stated herein. Statements regarding legal action have been reviewed and approved by the college attorney.

IV. WCC User Contract

I have read and agree to abide by the terms and conditions of the Wilkes Community College Computer Ethics Policy, and as such I am granted all the rights and privileges of computer use associated with this agreement by Wilkes Community College. I accept full responsibility for failure to comply with any or part of this agreement, and I acknowledge that willful misconduct and failure to maintain this contract may result in actions by Wilkes Community College. Actions may include fines for damages, temporary or permanent suspension of user rights, disciplinary actions as deemed necessary, and legal actions caused by failure to comply with copyright laws and licensing agreements.

Signature **Date**

Wilkes Community College
Ethical Instruction Plan

This guideline for appropriate computing behavior and ethical conduct consists of a sixteen week instructional plan for introducing ethical topics for class discussion. This module may be included within any existing computer course; however, an introductory computer course may be preferable. Each topic is introduced by the instructor and followed by class discussion. Each point listed below comes from the college's computer ethics policy. While students should have already read the policy and signed their student contract at the beginning of the semester, they may not fully understand all the ethical issues outlined in the policy. The purpose of this instructional unit is to provide students with an understanding of why ethical behavior is necessary and how to make the wisest decisions when faced with ethical dilemmas.

Ethical cases are provided by Oz's (1994) "Ethics: for the Information Age." According to Oz research shows that one of the most effective methods to teach ethics is to stimulate individual thinking and personal interpretation through the case based approach. The ethical cases place students in dilemmas that each must solve alone. There are no right or wrong answers provided with the cases; however, Oz does recommend using the utilitarian approach for the greatest good for the greatest number of people. While the class discussion topics are ordered, the ethical cases are in no direct order and may be arranged to suit individual instructor preferences.

Integrity and Accuracy

- Week 1: sharing user access or passwords, stealing passwords, or unauthorized accessing data
- Week 2: using computing resources for purposes other than those specified or originally intended
- Week 3: using computing resources for personal gain
- Week 4: knowingly transmitting or creating computer viruses
- Week 5: intercepting transmitted information, hacking into networks and systems, or cracking codes either on campus or from another location

Copyright and Licensing

- Week 6: engaging in software piracy, illegally copying of licensed software, or infringing upon software license agreements
- Week 7: loading, downloading from any source, copying or borrowing software that is in violation with existing licensing or laws
- Week 8: knowingly altering software belonging to the college that violates copyright laws and licensing agreements

Privacy

- Week 9: showing a lack of respect for the privacy and security of other users, data, or network system

- Week 10: borrowing, copying, examining, or removing another user's electronic mail, files, records, passwords, or personal property

Damages and Material Usage

- Week 11: monopolizing resources (playing games); wasting software, hardware, or supplies; using computing resources to commit crimes; theft or destruction of hardware and/or software

Internet and Electronic Mail

- Week 12: engaging in the displaying, downloading, and viewing of inappropriate, offensive or obscene materials
- Week 13: downloading shareware without compliance to payment and registration, or freeware that is permanently installed on the computer hard drive
- Week 14: engaging in the transmission of obscene, defamatory, harassing, offensive, annoying, or abusive e-mails
- Week 15: misrepresenting the college on the Internet or falsifying their identity
- Week 16: posting information on the Internet that violates the college code of conduct

Ethics Cases:

1. Luddonia And Summonia
2. Data Alteration
3. Worker Displacement
4. Monitoring E-Mail
5. Conflicts And Priorities
6. Obligations To Clients
7. High-Tech Diagnosis
8. Obligations To Employer
9. Miscommunications
10. Ethics In Higher Education
11. Ethics In Politics
12. Invasion Of Privacy
13. Fraud And Money Theft
14. First Amendment Rights
15. Obligations To Society
16. Confidentiality